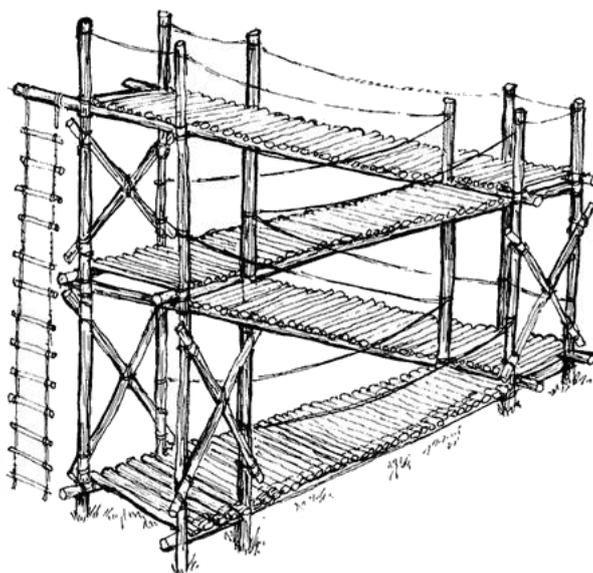


QUADERNO DI MATEMATICA

A. S. MATHESIS - SEZIONE BETTAZZI

A.A. 2010/2011

DISPENSE DI MATEMATICA OLIMPIONICA



A. Astolfi G. Audrito A. Carignano F. Tanturri

seconda edizione riveduta e ampliata da
G. Audrito G. Distefano R. Maffucci L. Prelli F. Roman

Associazione Subalpina Mathesis sezione Bettazzi



Ringraziamenti

Torino, 31/12/2007

Un ringraziamento speciale a Stefano Marò e Luca Clot per l'aiuto grafico e a Teresa Boggio, Francesco Giordano, Riccardo Maffucci, Marco Protto, Giovanni Rosso, Giangiacomo Sanna, Elisa de Vito, senza i quali sarebbe stato impossibile portare a termine questo progetto. Un doveroso ringraziamento anche all'Associazione Subalpina Mathesis che ha consentito la stampa di questi appunti, al suo presidente il professor Franco Pastrone, e al coordinatore del progetto il professor Pierluigi Pezzini.

Torino, 15/12/2010

Si ringraziano Giorgio Audrito, Fabio Roman, Lorenzo Prelli, Riccardo Maffucci e Gregory Distefano per l'opera di revisione e di integrazione che, a tre anni di distanza dal primo rilascio, ha permesso di realizzare una nuova edizione di queste dispense, rinnovata nella forma e arricchita nella sostanza, anche sulla base delle esperienze personali di tutti i ragazzi coinvolti in questo progetto di insegnamento giunto al suo quarto anno.

Come usare questo libro

Questo libro è stato pensato come supporto per lo studente che intende prepararsi per le olimpiadi della matematica, e cerca una solida base di teoria prima di affrontare i problemi proposti. Resta comunque accertato il fatto che, per ottenere buoni risultati alle olimpiadi, sia assolutamente necessario allenarsi con molti esercizi, per creare un occhio attento a discernere le diverse tipologie e strategie risolutive.

Gli argomenti teorici richiesti dalle olimpiadi della matematica sono, in buona parte, al di fuori dell'attuale programma ministeriale; eppure siamo convinti che possano essere di grande aiuto per lo sviluppo di una mentalità scientifica, deduttiva e creativa. Abbiamo quindi cercato di rivolgere questo libro ad un pubblico di studenti il più ampio possibile, conservando un'impostazione rigorosa ma rinunciando ad ogni inutile formalismo ed evidenziando in particolar modo gli aspetti applicativi.

Per iniziare un allenamento di tipo pratico, abbiamo inserito alcuni esercizi alla fine di ogni capitolo, di cui una parte con soluzione proposta nella parte finale del fascicolo; molti altri se ne possono trovare in [2], [3] e [4], raccolte di problemi proposti effettivamente in sede olimpica. Abbiamo scelto, alla fine di ogni capitolo, di segnalare alcuni esercizi presi da queste fonti, citando semplicemente la gara e il numero di esercizio corrispondente (nei riferimenti a [4]), o il codice numerico (nei riferimenti a [2] o [3]). Inoltre, tra le novità della nuova edizione, ogni capitolo si introduce con un problema, in modo tale da far ambientare subito il lettore con l'argomento, e accontentare i più desiderosi di passare subito alla pratica.

Infine abbiamo inserito, per chi fosse particolarmente interessato e volesse spingersi un po' oltre quelle che possono essere le ambizioni di base, alcuni paragrafi di approfondimento, nei quali vengono introdotti e affrontati alcuni argomenti più impegnativi e meno comuni, ma che possono comunque risultare utili nella risoluzione di problemi olimpionici, in particolare nelle fasi più avanzate della gara.

Buona lettura — e buone olimpiadi — a tutti!

Ringraziamenti		i
Come usare questo libro		iii
1 Logica e Matematizzazione		1
1.1	Connettivi logici	1
1.2	Principio dei cassetti (o della piccionaia)	3
1.3	Principio di induzione	4
1.3.1	Usi particolari del principio di induzione	4
1.4	Tabelle di verità	5
1.5	Teoria dei giochi	7
1.6	Invarianti	8
1.7	Colorazioni	9
1.8	Esercizi	10
1.8.1	Esercizi di base	10
1.8.2	Esercizi svolti	10
1.8.3	Esercizi proposti	11
2 Teoria dei Numeri		13
2.1	Operazioni e relazioni fondamentali	13
2.1.1	Divisione con resto	13
2.1.2	Divisibilità e primalità	14
2.1.3	MCD e mcm	15
2.1.4	Criteri di congruenza	16
2.2	Congruenze	17
2.2.1	Definizione	17
2.2.2	Somma e prodotto	18
2.2.3	Divisione e semplificazione	18
2.2.4	Operazioni ripetute	19
2.2.5	Residui quadratici	19
2.2.6	Sistemi di congruenze	20

2.2.7	Usò delle congruenze	21
2.3	Equazioni Diofantee	22
2.3.1	Equazioni diofantee di primo grado in due variabili	22
2.3.2	Metodo di scomposizione parziale	23
2.3.3	Metodo delle congruenze	24
2.4	Approfondimenti	26
2.4.1	Elevamento a potenza	26
2.5	Esercizi	28
2.5.1	Esercizi di base	28
2.5.2	Esercizi svolti	29
2.5.3	Esercizi proposti	30
3	Algebra	33
3.1	Successioni	33
3.1.1	Progressioni aritmetiche	34
3.1.2	Progressioni geometriche	34
3.1.3	Progressioni miste	35
3.2	Polinomi	35
3.2.1	Operazioni tra polinomi	36
3.2.2	Divisione euclidea tra polinomi	37
3.2.3	Scomponibilità di polinomi	37
3.2.4	Principio di identità dei polinomi	39
3.2.5	Radici razionali dei polinomi	39
3.2.6	Teorema di Ruffini	40
3.2.7	Relazioni tra radici e coefficienti dei polinomi	40
3.3	Disuguaglianze	41
3.3.1	Disuguaglianze tra le medie	41
3.3.2	Disuguaglianza di riarrangiamento	42
3.3.3	Disuguaglianza triangolare	42
3.4	Approfondimenti	43
3.4.1	Basi di numerazione	43
3.4.2	Dalla base b alla base 10	43
3.4.3	Dalla base 10 alla base b	43
3.4.4	Numeri decimali	44
3.4.5	Successioni per ricorrenza lineari	44
3.5	Esercizi	46
3.5.1	Esercizi di base	46
3.5.2	Esercizi svolti	47
3.5.3	Esercizi proposti	48
4	Combinatoria	51
4.1	Premesse per il calcolo combinatorio	52
4.2	Permutazioni	53
4.2.1	Permutazioni semplici	53
4.2.2	Permutazioni con ripetizione	53

4.3	Disposizioni	54
4.3.1	Disposizioni semplici	54
4.3.2	Disposizioni con ripetizione	54
4.4	Combinazioni	55
4.4.1	Combinazioni semplici	55
4.4.2	Combinazioni con ripetizione	56
4.5	Principio di inclusione-esclusione	56
4.6	Conteggi classici	57
4.7	Probabilità	59
4.7.1	Definizione	59
4.7.2	Probabilità di eventi composti	61
4.7.3	Probabilità condizionata e dell'intersezione	62
4.8	Approfondimenti	63
4.8.1	Valor medio	63
4.8.2	Periodo di una permutazione	64
4.9	Esercizi	66
4.9.1	Esercizi di base	66
4.9.2	Esercizi svolti	69
4.9.3	Esercizi proposti	71
5	Geometria	77
5.1	Teoremi	77
5.1.1	Angolo alla circonferenza	77
5.1.2	Angolo esterno	77
5.1.3	Bisettrice	77
5.1.4	Due corde	78
5.1.5	Euclide 1	78
5.1.6	Euclide 2	78
5.1.7	Secanti	78
5.1.8	Talete	78
5.2	Punti notevoli	78
5.2.1	Baricentro	78
5.2.2	Circocentro	79
5.2.3	Incentro	79
5.2.4	Ortocentro	80
5.3	Criteri	80
5.3.1	Criteri di congruenza	80
5.3.2	Criteri di similitudine	80
5.3.3	Criteri di circoscrittibilità e inscrittibilità	81
5.4	Formule per il calcolo geometrico	81
5.4.1	Diseguaglianza triangolare	81
5.4.2	Calcolo dell'area	81
5.4.3	Calcolo del volume	81
5.4.4	Raggi	82
5.4.5	Formula di Erone	82

5.4.6	Formula di Eulero	82
5.5	Approfondimenti	82
5.5.1	Calcolo sintetico	82
5.5.2	Calcolo trigonometrico	84
5.6	Esercizi	85
5.6.1	Esercizi svolti	85
5.6.2	Esercizi proposti	85
Soluzioni		89
6.1	Logica e Matematizzazione	89
6.2	Teoria dei Numeri	89
6.3	Algebra	91
6.4	Combinatoria	92
6.5	Geometria	95
Simboli e notazioni		99
Strategie euristiche		103
Tabelle riassuntive		105

La *logica*, nella classificazione dei problemi olimpici, include tutti i problemi che si basano sullo studio della verità di proposizioni, mentre la *matematizzazione* è il contenitore per tutti i problemi che non rientrano in nessun'altra categoria. I principali argomenti trattati sono tabelle di verità, giochi e colorazioni.

5 ragazzi A, B, C, D, E portano un cappellino di colore bianco o di colore rosso e ciascuno di loro non sa di che colore è il suo cappellino. Si sa che chi porta il cappellino rosso dice sempre la verità, mentre chi porta il cappellino bianco mente sempre.

A dice: *Io vedo tre cappellini rossi e uno bianco.*

B dice: *Io vedo quattro cappellini bianchi.*

C dice: *Io vedo un cappellino rosso e tre bianchi.*

D dice: *Io vedo quattro cappellini rossi.*

Determinare il colore del cappellino di ogni ragazzo.

1.1 Connettivi logici

Un *connettivo logico* è un operatore che lega fra loro due proposizioni A e B formando una terza proposizione C . Il valore vero o falso di C dipende dal valore di A , di B e dal connettivo logico usato. Vediamo i principali connettivi logici:

- la congiunzione logica *e*, in latino *et*, in inglese *and*, indicata con il simbolo \wedge .

A	B	$A \wedge B$
V	V	V
V	F	F
F	V	F
F	F	F

- la disgiunzione inclusiva *o*, in latino *vel*, in inglese *or*, indicata con il simbolo \vee .

A	B	$A \vee B$
V	V	V
V	F	V
F	V	V
F	F	F

- la disgiunzione esclusiva *o*, in latino *aut*, in inglese *xor*, indicata dal simbolo $\dot{\vee}$.

A	B	$A \dot{\vee} B$
V	V	F
V	F	V
F	V	V
F	F	F

- la negazione *non*, indicata dal simbolo \neg , che agisce su un'unica proposizione.

A	$\neg A$
V	F
F	V

- l'implicazione logica *se ... allora ...* indicata col simbolo \Rightarrow
 $A \Rightarrow B$ significa che se è vera A allora è sicuramente vera la B ma non dice niente se la frase A è falsa.

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

Dire quando la frase "Se piove allora ci sono le nuvole" è falsa.

La frase è falsa solo nel caso che piova ma non ci siano le nuvole, mentre rimane vera se non piove, che ci siano o no le nuvole.

- la coimplicazione *se e solo se* indicata col simbolo \Leftrightarrow .
 $A \Leftrightarrow B$ significa che se è vera A allora è sicuramente vera la B e viceversa, quindi le due proposizioni sono equivalenti a tutti gli effetti.

A	B	$A \Leftrightarrow B$
V	V	V
V	F	F
F	V	F
F	F	V

Dire quando la frase "Piove se e solo se cade acqua dal cielo" è vera.

La frase è vera in due casi, se piove e cade acqua dal cielo, oppure se non piove e non cade acqua dal cielo; in qualsiasi altro caso è falsa.

1.2 Principio dei cassetti (o della piccionaia)

Se si ripartisce un insieme di almeno n oggetti in $n - 1$ blocchi vi deve essere almeno un blocco che contiene più di un oggetto.

Di conseguenza se si ripartiscono $nk + 1$ oggetti in n blocchi, ci sarà almeno un blocco che contiene più di k oggetti.

Quante persone sono necessarie perché ce ne siano almeno 2 con il compleanno nella stessa data?

Ci sono 366 date di nascita possibili, quindi se ho 367 persone, due tra di loro sono sicuramente nate lo stesso giorno.

In un cassetto ho 6 paia di calze di 3 colori diversi, quante calze devo prendere per essere sicuro di averne 2 dello stesso colore, una sinistra e una destra?

Esaminiamo il caso peggiore: le prime 3 calze sono tutte di colore diverso, quindi con la quarta estrazione sono sicuro di averne 2 dello stesso colore. Però adesso potrei avere 3 calze dello stesso tipo delle prime 3. La settima calza invece sarà sicuramente di un colore che ho già estratto e si accoppierà sicuramente con una di quelle che ho già.

1.3 Principio di induzione

Spesso per dimostrare direttamente una proprietà dei numeri naturali si applica il *principio di induzione*, il cui enunciato è il seguente:

Sia P una proprietà qualunque scritta a partire da un numero naturale (per esempio *non c'è nessun animale con n zampe*). Se si dimostra che:

- a) la proprietà P vale per 0
- b) e che se vale per n , vale anche per $n + 1$

allora la proprietà P vale per ogni numero naturale.

Dimostriamo che $n^3 - n$ è divisibile per 6 qualunque sia n .

- a) $0^3 - 0 = 0$, che è ovviamente divisibile per 6
- b) Dimostriamo che se $n^3 - n$ è divisibile per 6 (ipotesi) anche $(n + 1)^3 - (n + 1)$ è divisibile per 6 (tesi).

$$(n + 1)^3 - (n + 1) = n^3 + 3n^2 + 3n + 1 - n - 1 = n^3 - n + 3n(n + 1)$$

$n^3 - n$ è divisibile per 6 per ipotesi

$3n(n + 1)$ è certamente divisibile per 3, ma anche per 2, essendo $n(n + 1)$ il prodotto di due numeri consecutivi (quindi sicuramente pari).

Quindi siccome se vale per n vale anche per $n + 1$, se vale per 0, vale anche per 1, ma se vale per 1, vale anche per 2, etc. quindi vale per tutti i numeri naturali.

1.3.1 Usi particolari del principio di induzione

Il principio di induzione si può utilizzare anche per ottenere una parte dei numeri naturali e non tutti, per esempio in questo modo:

1. a) la proprietà P vale per 0
 - b) e se vale per n , vale anche per $n + 2$
 quindi la proprietà P vale per tutti i pari.

2. a) la proprietà P vale per 1
 - b) e se vale per n , vale anche per $n + 2$
 quindi la proprietà P vale per tutti i dispari.

Ma se vale per tutti i pari e tutti i dispari, allora vale per tutti gli n .

Inoltre il primo valore non deve per forza valere 0, una certa regola potrebbe essere in fatti dimostrata per qualunque n a partire da un certo k in poi:

- a) la proprietà P vale per k
- b) e se vale per n , vale anche per $n + 1$

Allora P vale per qualsiasi $n > k$

Allo stesso modo il passo induttivo b) non deve per forza essere $n + 1$ ma può essere $n - 1$:

- a) la proprietà P vale per k
- b) e se vale per n , vale anche per $n - 1$

la proprietà P è dimostrata per tutti gli $n < k$.

1.4 Tabelle di verità

Per venire a capo della maggior parte dei problemi logici, ovvero quelli in cui un'affermazione può essere vera o falsa, la migliore strategia è la realizzazione di una tabella di verità. Questa tabella serve per esaminare ordinatamente tutti i casi possibili, escludendo le contraddizioni.

Occorre costruire una tabella che contiene, nella prima riga (o colonna) le affermazioni, nelle successive il possibile valore di verità (vero o falso). Cominciando da sinistra verso destra, si suppone un'affermazione vera (o falsa) e se ne deducono le altre. Se si arriva ad una contraddizione l'ipotesi è da scartare (in questo caso la verità o la falsità della prima affermazione) e di conseguenza la prima affermazione è necessariamente falsa (o, rispettivamente, vera). Stabilito ciò, si può passare ad un'altra affermazione, in genere la seconda. L'esame di tutte le possibilità che si possono verificare è spesso sufficiente per rispondere al problema.

Nel registrare le dichiarazioni dei tre imputati ad un processo, il cancelliere è stato piuttosto trascurato, e dal verbale risulta quanto segue:

Carlo: il colpevole è ...ario.

Dario: il colpevole è Dario.

Mario il colpevole è ...ario.

Sapendo che il colpevole ha mentito e almeno uno degli innocenti ha detto la verità, che cosa si può concludere?

- A) *il colpevole è Dario*
- B) *non si può determinare il colpevole*
- C) *Carlo accusato Dario*
- D) *Mario ha accusato Dario*
- E) *Mario ha accusato Mario*

Costruiamo una tabella di verità per risolvere questo problema partendo dall'affermazione di Dario che è l'unica completa.

Frase	valore	Dario	Mario	Carlo
Il colpevole è Dario	V	C		

Ma questo è assurdo perché la frase è stata detta da Dario, che se fosse stato colpevole avrebbe dovuto mentire.

Frase	valore	Dario	Mario	Carlo
Il colpevole è Dario	V	C		Assurdo
Il colpevole è Dario	F	I		

Questa riga è sicuramente l'unica possibilità corretta, cioè Dario è un innocente che mente. Passiamo quindi ad un'altra affermazione:

Frase	valore	Dario	Mario	Carlo
Il colpevole è Dario	V	C		Assurdo
Il colpevole è Dario	F	I		Sicuro
Il colpevole è ...ario	V	I

A questo punto bisogna dividere i casi, in chi ha detto la frase e qual'era la lettera che manca.

Partiamo da Carlo, sappiamo già che non può accusare Dario perché Dario è innocente e noi abbiamo supposto l'affermazione vera, quindi accusa Mario.

Frase	valore	Dario	Mario	Carlo
Il colpevole è Dario	V	C		Assurdo
Il colpevole è Dario	F	I		Sicuro
Il colpevole è (M)ario	V	I	C	I

Quindi Mario, che non può auto accusarsi ha accusato Dario, mentendo. Questa è una soluzione al problema ma non è detto che sia l'unica.

Se Carlo mente è sicuramente colpevole (perché almeno uno dice la verità) ma allora mente anche Mario, il che è assurdo. In questo caso non dobbiamo neanche andare a considerare qual'è la lettera non scritta perché la deduzione si basa su quelle che abbiamo.

Frase	valore	Dario	Mario	Carlo
Il colpevole è Dario	V	C		Assurdo
Il colpevole è Dario	F	I		Sicuro
Il colpevole è (M)ario	V	I	C	I
Il colpevole è ...ario	F	I	I	C

La configurazione di prima risulta quindi l'unica possibile, quindi la soluzione giusta è la (D), Mario colpevole, mente accusando Dario.

Soluzione problema di inizio capitolo.

Se E porta un cappellino bianco, allora D mente e porta un cappello bianco. In questo caso ci sarebbero 2 cappellini bianchi, quindi A mente e porta un cappellino bianco.

Se C dice la verità, allora C ha un cappellino rosso e B vede un cappellino rosso, quindi B mente. Allora B porta un cappellino bianco, in contraddizione con C .

Se invece C mente, allora ha un cappellino bianco. Quindi A , C , D , E portano cappelli bianchi, concordemente a B ma in contraddizione con il fatto che C è un mentitore.

Pertanto E deve portare un cappellino rosso. Ciò implica che B è un mentitore, dunque ha un cappello bianco. Ma allora anche D mente, e dunque A dice la verità e ha un cappello rosso. In conclusione, la sola soluzione possibile è che A , B , D abbiano cappellini bianchi, mentre C ed E l'abbiano rosso.

1.5 Teoria dei giochi

In matematica si intende per gioco una qualunque situazione in cui un qualsiasi numero di giocatori compie delle mosse. Nelle olimpiadi di matematica, solitamente, si trovano solo due tipi di giochi: i giochi a due giocatori in cui la lista di mosse è in comune, nei quali bisogna trovare una strategia vincente, e i solitari, in cui occorre capire se si può passare da una configurazione di partenza a una configurazione finale.

Nei giochi a due, normalmente per capire quando uno o l'altro può vincere, il modo migliore di procedere è al contrario: ci si chiede quando un giocatore è sicuro di perdere a partire da casi semplici e poi cercando di generalizzare. In questo modo si realizza una lista di situazioni perdenti (e che di conseguenza sono vincenti per l'avversario).

Il passo successivo è capire come si può lasciare l'avversario in una situazione perdente. Proseguendo in questo modo si ottiene una lista spaccata a metà con situazioni vincenti da una parte e situazioni perdenti dall'altra, e una lista di mosse per lasciare l'avversario sempre in una situazione perdente, questa seconda lista viene chiamata strategia vincente.

Un gioco che fanno Alice e Barbara ha le seguenti regole: ci sono n dischi messi in fila. A turno (comincia Alice) il giocatore toglie un numero a scelta da 1 a 7 di dischi. Vince chi toglie l'ultimo disco.

Per quali n Alice vince se gioca bene? Per quali n Barbara vince se gioca bene?

Chiaramente chi si trova tra 1 e 7 dischi ha vinto perché può toglierli tutti, mentre chi se ne trova 8 perde sicuramente perché deve lasciarne all'altro un numero compreso tra 1 e 7. Chi si trova tra 9 e 15 dischi può toglierne un numero tale da lasciarne all'altro 8 e quindi vince. Per 16 invece capita quello che capitava con 8. Diventa quindi chiaro

che vince il primo che gioca (Alice) se n non è un multiplo di 8, vince Barbara se lo è. La strategia vincente è di lasciare all'avversario sempre un multiplo di 8.

1.6 Invarianti

In generale la parola *invariante* indica una proprietà che non cambia durante la risoluzione del problema, o che cambia in modo molto facile da determinarsi. Questo permette di capire come funziona un gioco anche quando le regole sono troppo complicate per trovare le situazioni a tentativi e poi generalizzare. Infatti una volta trovato l'invariante possiamo considerare come si svolge il gioco, e in particolare come si comportano le possibili mosse, solo in relazione a quell'invariante.

Alice e Bob fanno il seguente gioco. Su una lavagna vi è scritto un intero $n > 1$, e a turno i due sfidanti devono fare una delle seguenti mosse:

- a) *Togliere 1 dall'intero n e passare,*
- b) *Oppure, se il numero $n \geq 10$, cancellare una cifra a caso dal numero e raddoppiare il risultato ottenuto. Per esempio, se $n = 158$, è possibile cancellare la cifra 5 e passare all'avversario il numero $36 = 18 \cdot 2$.*

Il gioco termina quando un giocatore riceve $n = 0$ e vince. Quale giocatore ha una strategia vincente, al variare di n ?

Per capire la strategia vincente, consideriamo l'invariante "la parità di n ". Questa quantità non è rigorosamente un invariante, tuttavia varia in maniera abbastanza semplice: infatti se n è dispari, qualunque delle due mosse restituirà un numero pari, mentre se è pari (e $n > 10$), possiamo scegliere se lasciare all'avversario un numero pari o dispari. A questo punto, chi si ritrova un numero pari sceglierà sempre la mossa a), così da lasciare all'avversario un numero dispari e riottenere quindi dopo un numero pari, fino a vincere raggiungendo lo 0 (che è pari). Ricapitolando, se n è pari vince Alice, mentre se n è dispari vince Bob.

Gli invarianti diventano poi lo strumento di soluzione fondamentale per un tipo particolare di giochi, i *solitari*.

Alberto per sconfiggere la solitudine ha inventato un gioco. All'inizio vi sono n bastoncini in pila, e poi Alberto può fare una di queste tre mosse:

- a) *Scegliere una pila con almeno 4 bastoncini e spezzarla in 4 pile;*
- b) *Scegliere una pila con y bastoncini, toglierle un numero di bastoncini $k \leq \frac{y}{2}$ e spostarli su un'altra pila;*
- c) *Scegliere una pila con almeno 2 bastoncini, spezzarla in 2 pile e quindi aggiungere una nuova pila con 5 bastoncini.*

Alberto vuole, mediante solo queste mosse, raggiungere una configurazione in cui tutte le pile hanno un solo bastoncino. Per quali n Alberto può vincere la partita? Con che strategia?

Chiamiamo n il numero totale di bastoncini presenti su tutte le pile, e m il numero di pile. All'inizio, $m = 1$ ed n è assegnato, alla fine $n' = m'$. Esaminamo come agiscono su questi due valori le varie mosse.

a) n non varia mentre $m' = m + 3$.

b) n ed m restano entrambi invariati;

c) $n' = n + 5$ ed $m' = m + 2$.

A questo punto si può notare come l'espressione $(n - m) \bmod 3$ sia un invariante in questo gioco; imponendo quindi che resti uguale all'inizio e alla fine abbiamo che $(n - 1) \bmod 3 = (n' - m') \bmod 3 = 0 \implies n \equiv 1 \pmod{3}$.

Resta poi solo da verificare che ogniqualvolta $n \equiv 1 \pmod{3}$ il gioco ha effettivamente soluzione; ma questa soluzione si ottiene semplicemente applicando ripetutamente la mossa a) ogni volta creando 3 nuove pile con 1 bastoncino l'una.

1.7 Colorazioni

Per risolvere alcuni problemi di *tassellazioni*, cioè quei problemi in cui dobbiamo ricoprire delle figure geometriche con dei "tasselli" di dimensioni e forma assegnate, è fortemente consigliato ricorrere alle colorazioni, che sono uno dei metodi per trovare degli invarianti. Questo è uno strumento potente e permette di risolvere problemi molto complessi, tuttavia in queste dispense vi è solo l'uso di base che se ne può fare. Supponiamo di avere un certo numero di quadretti che formano una certa figura e supponiamo di chiederci se sia possibile o meno ricoprire questa figura con tasselli di una data forma. Chiaramente, se i tasselli contengono n quadretti l'uno, il totale dei quadretti da riempire dovrà essere multiplo di n . Tuttavia questa è una condizione necessaria ma ben lontana dall'essere sufficiente. Spesso è molto lungo e difficile trovare uno dei riempimenti possibili. Può essere invece più facile dimostrarne l'impossibilità con l'uso delle colorazioni.

Innanzitutto si colora regolarmente (come una scacchiera, ad esempio, ma anche in altri modi) la figura di partenza. Successivamente si prova ad inserire il tassello sulla figura da riempire e si valuta quante e quali caselle possano essere ricoperte: infine si trova una qualche ragione per cui tasselli di quel genere non possono ricoprire tutta la figura di partenza (è più facile a farsi che a dirsi!).

Si consideri un quadrato 10×10 quadretti a cui sono stati tolti due quadrettini ad angoli opposti. Dimostrare che non è possibile ricoprire questa figura con pezzi 2×1 .

Coloriamo il quadrato a scacchi. Nel quadrato completo il numero di quadratini bianchi e quello di quadratini neri è lo stesso ma se togliamo quelli ai due angoli opposti, essendo questi due dello stesso colore (supponiamo nere), avremo che i quadrati bianchi

sono 2 in più. Ogni pezzo 2×1 copre obbligatoriamente una casella bianca e una nera. Da qui l'impossibilità di coprire tutte le caselle.

1.8 Esercizi

1.8.1 Esercizi di base

1. Quanti numeri della tombola devi prendere per averne con certezza uno pari?
2. Quanti lanci di un dado devi fare per essere sicuro che sia uscita 12 volte una stessa faccia?
3. Dimostra per induzione che $n^2 > 10n$ per n grandi.
4. Dimostra che la somma dei primi n quadrati è $n(n+1)(2n+1)/6$
5. Dimostra che la somma dei primi n cubi è $[n^2(n+1)^2]/4$

1.8.2 Esercizi svolti

1. Dimostra che scegliendo 5 punti all'interno di un quadrato di lato 10 cm ce ne sono sempre almeno due con distanza inferiore a $5\sqrt{2}$.
2. 100 lampadine sono disposte in modo da formare un pannello quadrato di 10 righe per 10 colonne. Alcune di esse sono accese, le altre sono spente. L'impianto elettrico è tale che quando si preme il pulsante che serve ad accendere (o spegnere) una lampadina, cambiano di stato (cioè si accendono o si spengono) anche tutte le lampadine che si trovano sulla sua colonna e quelle che si trovano sulla sua riga. Partendo da quali configurazioni, operando in modo opportuno, è possibile fare in modo che alla fine tutte le lampadine risultino accese?
3. Marco e Roberto hanno una tavoletta di cioccolato formata da 8 quadretti di cui il quadretti d'angolo, in alto a sinistra non è buono. Decidono allora di giocare a questo gioco. Ad ogni turno ogni giocatore spezza in due la cioccolata lungo una delle linee di separazione tra i quadretti, e poi si mangia la parte che non contiene il quadretto cattivo. Vince chi lascia all'avversario il solo quadretto cattivo. Sapendo che Roberto è il primo a giocare, cosa deve mangiare per essere sicuro della vittoria?

(A) I due quadretti più a destra.
(B) I quattro quadretti più a destra.
(C) I sei quadretti più a destra.
(D) I quattro quadretti in basso.
(E) Qualunque mossa faccia, Roberto perde.
4. Quattro ruote a, b, c, d hanno i centri nei vertici di un quadrato, i raggi rispettivamente di 14, 15, 16 e 18 cm e sono collegate esternamente da una cinghia in modo che il sistema possa ruotare senza che la cinghia possa slittare. Dopo quanti giri della ruota a il sistema torna per la prima volta nella posizione iniziale?

1.8.3 Esercizi proposti

1. Ci sono n persone. Dimostra che durante la festa almeno 2 persone hanno stretto lo stesso numero di mani.
2. Dimostra che ogni quadrato è scomponibile in k quadrati con $k \geq 6$.

3. Dimostra che è possibile riempire con pezzi  un quadrato di lato 2^n a cui è stata tolta una casella.

4. Alcuni matematici hanno studiato i numeri naturali "speciali" (di cui ignoriamo la definizione) ed hanno dimostrato i teoremi sotto elencati. Uno di essi implica tutti gli altri. Quale?

- (A) Ci sono infiniti numeri dispari che non sono speciali.
- (B) Ci sono infiniti numeri dispari e infiniti numeri pari che non sono speciali.
- (C) Per ogni numero speciale s c'è un numero naturale n non speciale tale che $n > s$.
- (D) C'è solo un numero finito di numeri speciali dispari.
- (E) Un numero speciale non può avere più di 1000 cifre.

5. Un giornalista deve fare un articolo su una classica isola di furfanti e cavalieri, in cui tutti gli abitanti o mentono sempre (e sono furfanti) o dicono sempre la verità (e sono cavalieri), e tutti si conoscono reciprocamente. Supponiamo che il giornalista intervisti una e una sola volta tutti gli abitanti dell'isola ed ottenga nell'ordine le seguenti risposte.

A_1 : "sull'isola c'è almeno un furfante"

A_2 : "sull'isola ci sono almeno 2 furfanti"

...

A_{n-1} : "sull'isola ci sono almeno $n - 1$ furfanti"

A_n : "sull'isola ci sono almeno n furfanti"

Può il giornalista stabilire se sull'isola ci sono più furfanti o più cavalieri?

6. Un treno fa la spola tra due città A e B che distano 20 km; di solito rispetta rigorosamente l'orario viaggiando a velocità costante. Un giorno, a metà strada tra A e B , viene fermato per tre minuti da un semaforo e riesce comunque ad arrivare in orario aumentando di 10 km/h la sua velocità nel tratto rimanente. Se avesse perso cinque minuti al semaforo, di quanto invece, avrebbe dovuto aumentare la sua velocità di marcia per arrivare in orario?
7. Un'isola ha la forma di un poligono convesso con perimetro di p km. Le acque territoriali si estendono fino a una distanza di b km dalla costa. Qual è l'area A delle acque territoriali e quale la lunghezza l della curva che la delimita?

8. Alice e Bob fanno un gioco molto divertente. Da un foglio di carta quadrettata ritagliano un rettangolo $m \times n$, dopodiché a turno (iniziando da Alice) ognuno di loro deve tagliare il rettangolo in due rettangoli (il taglio deve essere orizzontale o verticale, e rispettare i quadretti), scartarne uno e passare l'altro al giocatore successivo. Chi riceve il rettangolo 1×1 perde. Chi vince, e come? Come cambia il gioco se sono costretti a scartare il rettangolo più piccolo?
9. Si vuole costruire una griglia di ferro con dei tondini a forma di 'L', con i due segmenti perpendicolari della stessa lunghezza. Due tondini non possono sovrapporsi, e nessuno di loro può debordare dalla griglia. Per quali valori dei lati del reticolo è possibile costruire una griglia del genere?
10. Un castello è composto da sette piani, ognuno con nove stanze disposte 3×3 . Un principe deve entrare da una delle quattro stanze 'centrali' del piano terra e salvare la principessa che si trova nella stanza corrispondente all'ingresso dell'eroe ma all'ultimo piano. Il principe per salvare la principessa deve attraversare tutte le stanze e raccogliere in ognuna una perla in esse contenute, senza passare due volte per la stessa camera. Sapendo che da ogni stanza è possibile raggiungere quelle adiacenti, riuscirà il principe a salvare la principessa?

La *teoria dei numeri*, nella classificazione dei problemi olimpici, si occupa dello studio delle proprietà dei numeri interi; e quindi di divisibilità, primalità, ed equazioni a valori interi.

Cinque uomini fanno naufragio su un'isola; non c'è nulla da mangiare tranne noci di cocco. Essi vanno a dormire ripromettendosi di dividersele la mattina seguente. Nel mezzo della notte, uno dei naufraghi sente improvvisamente fame e decide di prendersi subito la sua parte di noci di cocco. Nel farlo, scopre che se ne toglie una sono esattamente divisibili per cinque. Decide pertanto di dare una noce di cocco ad una scimmia che si trova nei paraggi e di prendersi la sua parte. Durante la notte, ognuno degli altri marinai fa la stessa cosa all'insaputa dell'altro, e ognuno trova un numero di noci di cocco che diventa divisibile per cinque una volta donata una noce di cocco alla scimmia. Al mattino, decidono come d'accordo di dividere il mucchio delle noci in parti uguali, e ne trovano ancora una di resto da lasciare alla scimmia. Quante erano all'inizio, come minimo, le noci di cocco?

2.1 Operazioni e relazioni fondamentali

2.1.1 Divisione con resto

Tra i numeri interi si possono svolgere le operazioni di somma, sottrazione e prodotto senza incontrare particolari difficoltà, nei modi noti a tutti. Più delicato è il problema della divisione, poiché è in generale impossibile svolgerla, se non si vuole sconfinare nei numeri razionali. Viene quindi introdotta una nuova operazione, la *divisione con resto*, per esprimere la divisione tra soli numeri interi.

Dati gli interi $a \neq 0$ e b , la divisione con resto di b per a associa a questi due numeri gli interi q ed r tali che:

$$b = a \cdot q + r, \quad 0 \leq r < a$$

Qualunque siano a e b , gli interi q ed r che soddisfano queste relazioni esistono e sono unici; q è detto *quoziente* ed r è detto *resto*.

Per meglio comprendere il significato della divisione con resto è utile immaginarsi l'operazione in un modo alternativo. L'intero q può essere ottenuto come il risultato della divisione esatta di b per a arrotondato per difetto, e considerando che la divisione esatta richiede di trovare il numero q tale che $aq = b$, il resto r rappresenta intuitivamente la misura dell'errore commesso nell'arrotondamento per difetto: infatti $r = b - aq$, cioè quanto i due lati dell'uguaglianza precedente discostano tra loro.

Dato che la divisione con resto restituisce due valori, per indicarla vengono usate due distinte scritture. Mantenendo le lettere della definizione, avremo che $b \operatorname{div} a = q$ restituisce il quoziente (divisione intera), mentre $b \operatorname{mod} a = r$ restituisce il resto (modulo).

- a) $7 \operatorname{div} 3 = 2$, $7 \operatorname{mod} 3 = 1$. Infatti $7 = 6 + 1 = 3 \cdot 2 + 1$, come nella definizione. Più intuitivamente $7/3 \simeq 2.33$ da cui per difetto $q = 2$, e infine il resto è dato da $r = 7 - 3 \cdot 2 = 7 - 6 = 1$, l'errore commesso.
- b) $37569 \operatorname{div} 100 = 375$, $37569 \operatorname{mod} 100 = 69$
- c) $60 \operatorname{div} 7 = 8$, $60 \operatorname{mod} 7 = 4$
- d) $-60 \operatorname{div} 7 = -9$, $-60 \operatorname{mod} 7 = 3$
- e) $-60 \operatorname{div} -7 = 9$, $-60 \operatorname{mod} -7 = 3$
- f) $60 \operatorname{div} -7 = -8$, $60 \operatorname{mod} -7 = 4$

2.1.2 Divisibilità e primalità

Si dice che a divide b , o che a è divisore di b , o che b è multiplo di a (in simboli $a \mid b$) se effettuando la divisione con resto di b per a si ottiene che $r = 0$. Più esplicitamente, $a \mid b$ se esiste un intero q tale che $b = aq$. Notare che tra i divisori di un numero b sono sempre presenti 1 e b stesso e che tutti i numeri dividono lo 0. Com'è facile verificare, la caratteristica di "essere multipli" si preserva con le combinazioni lineari: in altre parole se a, b sono multipli di d allora $h \cdot a + k \cdot b$ è anche multiplo di d per qualsiasi scelta di h, k interi.

Si dice inoltre che p è un numero primo se ogniquale volta divide un prodotto divide anche almeno uno dei fattori, cioè $p \mid ab \Rightarrow p \mid a \vee p \mid b$. Ai nostri fini, questa definizione è equivalente a quella più nota, secondo cui un numero è primo se non ha divisori all'infuori di 1 e se stesso. Notare che 1 non è considerato un numero primo.

I numeri primi hanno un ruolo particolare nella teoria dei numeri, soprattutto poiché ogni intero è scrivibile in modo unico come prodotto di potenze di numeri p_i primi distinti:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

La scomposizione in fattori primi di un numero può essere utilmente scritta indicando i fattori $p_i^{\alpha_i}$ per tutti i primi in ordine di grandezza, ponendo $\alpha_j = 0$ per i primi p_j non presenti nella scomposizione. Per esempio, $6776 = 2^3 \cdot 7 \cdot 11^2 = 2^3 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^2 \cdot 13^0 \cdot \dots$

Verificare se un numero a è primo o meno è un problema complesso, tuttavia sono note alcune strategie per farlo. Una prima strategia (utile anche per trovare la fattorizzazione di un numero non primo) consiste nel dividere il numero a per tutti i primi noti in ordine crescente, fino ad arrivare a \sqrt{a} . A quel punto, se nessuno dei primi che abbiamo provato era un divisore esatto di a , allora a è certamente primo (infatti se possiede un divisore $d > \sqrt{a}$, possiede anche il divisore $a/d < \sqrt{a}$).

La seconda strategia (nota con il nome di *crivello di Eratostene*) serve invece per trovare tutti i primi da 2 fino a un certo limite prefissato L . Si scrivono in tabella tutti i numeri da 2 a L , poi si parte da 2, si dice che è primo e si cancellano dalla tabella tutti i suoi multipli (che certamente non sono primi). A questo punto si prende il successivo numero non ancora cancellato (che è il 3), e si cancellano tutti i suoi multipli, e così via cancellando i multipli di tutti i primi che si trovano con questo procedimento. I numeri primi, alla fine, saranno proprio quelli che non sono stati cancellati.

Infine, è spesso utile sfruttare i numeri primi per trovare i divisori di un numero: dato un numero $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, i suoi divisori sono tutti i numeri la cui scomposizione utilizza gli stessi primi p_i di n , con esponenti inferiori o uguali.

2.1.3 MCD e mcm

Dati a e b , si dice *minimo comune multiplo* quell'intero $l = \text{mcm}(a, b)$ che è multiplo sia di a che di b ed è divisore di ogni altro numero con questa proprietà (equivalentemente, è il più piccolo tra i multipli sia di a che di b). Similmente, si dice *massimo comun divisore* quell'intero $g = \text{MCD}(a, b)$ che divide sia a che b ed è multiplo di ogni altro numero con questa proprietà (equivalentemente, è il più grande tra i divisori comuni di a e b). Due numeri, infine, si dicono *coprimi* se $\text{MCD}(a, b) = 1$. Per esempio, $\text{mcm}(4, 6) = 12$ e $\text{MCD}(4, 6) = 2$; mentre $\text{mcm}(10, 21) = 210$ e $\text{MCD}(10, 21) = 1$, quindi i due numeri sono coprimi.

È semplice calcolare questi valori nel caso in cui sia nota la scomposizione in fattori primi dei due interi $a = \prod p_i^{\alpha_i}$ e $b = \prod p_i^{\beta_i}$. In questo caso infatti la scomposizione del minimo comune multiplo si ottiene prendendo per ogni primo p_i il massimo tra gli esponenti α_i e β_i (assumendo 0 ad esponente per i primi non presenti); mentre la scomposizione del massimo comun divisore si ottiene prendendo per ogni primo p_i il minimo tra gli stessi esponenti α_i e β_i (assumendo sempre 0 ad esponente per i primi non presenti).

$$\text{mcm}(a, b) = \prod_i p_i^{\max(\alpha_i, \beta_i)}$$

$$\text{MCD}(a, b) = \prod_i p_i^{\min(\alpha_i, \beta_i)}$$

Per esempio, $\text{mcm}(2^5 \cdot 5, 2^3 \cdot 3) = 2^5 \cdot 3 \cdot 5 = 480$ e $\text{MCD}(2^5 \cdot 5, 2^3 \cdot 3) = 2^3 = 8$. Sfruttando la proprietà precedente, e considerando che $a + b = \min(a, b) + \max(a, b)$, è facile dimostrare l'importante relazione $\text{mcm}(a, b) \cdot \text{MCD}(a, b) = a \cdot b$.

Per calcolare l'MCD (e di conseguenza, tramite la relazione precedente, anche l'mcm) anche nel caso di numeri grandi di cui non si conosce la scomposizione in fattori primi, è utile il

seguinte *algoritmo di Euclide*:

$$MCD(a, b) = MCD(b, a \bmod b)$$

L'algoritmo consiste, in pratica, nell'applicare più volte la divisione con resto e alla fine ricavare il risultato tramite il fatto che $MCD(a, 0) = a$ per ogni intero a .

I freni della macchina di Alberto si guastano regolarmente ogni 34 giorni; lui però usa la sua macchina solo ogni 44 giorni. Ogni quanti giorni Alberto è costretto a compiere un incidente?

È sufficiente calcolare il $mcm(34, 44)$. Per farlo calcoliamo prima l'MCD:

$$\begin{aligned} MCD(34, 44) &= \\ &= MCD(44, 34 \bmod 44) = MCD(44, 34) = \\ &= MCD(34, 44 \bmod 34) = MCD(34, 10) = \\ &= MCD(10, 34 \bmod 10) = MCD(10, 4) = \\ &= MCD(4, 10 \bmod 4) = MCD(4, 2) = \\ &= MCD(2, 4 \bmod 2) = MCD(2, 0) = 2 \end{aligned}$$

e poi calcoliamo $mcm(34, 44) = \frac{34 \cdot 44}{MCD(34, 44)} = \frac{34 \cdot 44}{2} = 748$.

Per finire, citiamo il noto *Teorema di Bezout*: dati due interi qualunque a e b , gli interi ottenibili come combinazioni lineari dei due (cioè come $h \cdot a + k \cdot b$ al variare di h e k interi qualunque) sono tutti e soli i multipli del massimo comun divisore (a, b). I coefficienti h e k che consentono di ricavare esattamente il massimo comun divisore sono spesso non facili da trovare, anche se è solitamente possibile procedere per tentativi.

2.1.4 Criteri di congruenza

Per calcolare il risultato dell'operazione modulo esistono alcuni utili criteri che sveltiscono i calcoli:

- Ogni intero modulo 2^n è uguale alle sue ultime n cifre modulo 2^n . Quindi, un numero è divisibile per 2^n solo se lo sono le sue ultime n cifre. Per esempio, $3367882 \bmod 8 = 882 \bmod 8 = 2$.
- Analogamente, ogni intero modulo 5^n è uguale alle sue ultime n cifre modulo 5^n ; ed è divisibile per 5^n solo se lo sono le sue ultime n cifre. Per esempio, $3367882 \bmod 25 = 82 \bmod 25 = 7$.
- Ogni intero modulo 3 o 9 è uguale alla somma delle sue cifre modulo 3 o 9. Per esempio, $3367882 \bmod 9 = 37 \bmod 9 = 10 \bmod 9 = 1$.

- Ogni intero modulo 11 è uguale alla somma delle sue cifre di posto dispari meno la somma delle sue cifre di posto pari modulo 11. Per esempio, $3367882 \bmod 11 = [(2 + 8 + 6 + 3) - (8 + 7 + 3)] \bmod 11 = (19 - 18) \bmod 11 = 1$. Notare che la cifra di posto 1 è quella delle unità.
- Un intero n è divisibile per 7, cioè $n \bmod 7 = 0$, se e solo se lo è il numero ottenuto dall'intero iniziale senza la cifra delle unità sottraendo due volte la cifra delle unità. Per esempio, $3367882 \bmod 7 = 0$ in quanto $336788 - 2 \cdot 2 = 336784$, e ripetendo $33678 - 2 \cdot 4 = 33670$, $3367 - 2 \cdot 0 = 3367$, $336 - 2 \cdot 7 = 322$, $32 - 2 \cdot 2 = 28$; ma dato che l'ultimo è divisibile per 7, lo sono anche tutti gli altri e in particolare il numero di partenza. Inoltre $394 \bmod 7 \neq 0$ in quanto $39 - 2 \cdot 4 = 31 \bmod 7 = 3 \neq 0$. Notare che questo criterio *non* è un criterio di congruenza: infatti $394 \bmod 7 = 2$ e non 3.
- Un intero n è divisibile per un numero a non primo se e solo se è divisibile per ciascuno dei fattori p^α della scomposizione in fattori primi di a .

Non è difficile dimostrare la veridicità di questi criteri, sfruttando il fatto che per definizione ogni numero $C_n C_{n-1} \dots C_2 C_1 C_0$ scritto in notazione decimale corrisponde a:

$$C_n C_{n-1} \dots C_2 C_1 C_0 = C_n \cdot 10^n + C_{n-1} \cdot 10^{n-1} + \dots + C_2 \cdot 10^2 + C_1 \cdot 10^1 + C_0 \cdot 10^0$$

2.2 Congruenze

2.2.1 Definizione

Due interi a e b si dicono *congrui* modulo m (in formule $a \equiv b \pmod{m}$) se divisi per m danno lo stesso resto. Equivalentemente, due interi sono congrui modulo m se $m \mid (a - b)$. Notare che una congruenza non è altro che un'uguaglianza tra resti, quindi dire $a \equiv b \pmod{m}$ equivale a $a \bmod m = b \bmod m$. Pertanto tutte le proprietà delle congruenze si rifletteranno in analoghe proprietà dell'operazione modulo.

È facile verificare che la congruenza rispetto a un modulo fissato è una relazione di equivalenza, e cioè che valgono le tre proprietà riflessiva ($a \equiv a \pmod{m}$), simmetrica (se $a \equiv b \pmod{m}$, allora $b \equiv a \pmod{m}$) e transitiva (se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, allora $a \equiv c \pmod{m}$). Per questo motivo è possibile definire il concetto di *classe di congruenza*: si definisce classe di congruenza di a modulo m (e si indica con $[a]$ o \bar{a}) l'insieme di tutti gli interi che divisi per m danno lo stesso resto di a . poiché i resti possibili sono tutti gli interi tra 0 ed $m - 1$, avremo m differenti classi di congruenza. Per esempio, modulo 4 avremo le classi:

$$\bar{0} = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

$$\bar{1} = \{\dots, -7, -3, 1, 5, 9, \dots\}$$

$$\bar{2} = \{\dots, -6, -2, 2, 6, 10, \dots\}$$

$$\bar{3} = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

Notare che ogni classe può essere chiamata con infiniti nomi diversi, uno per ogni elemento che contiene; per esempio nel caso precedente avevamo $[1] = [9] = \dots$

2.2.2 Somma e prodotto

Le congruenze si comportano bene rispetto a somma, sottrazione e prodotto. Infatti:

$$a \equiv b, \quad c \equiv d \pmod{m} \implies$$

$$a + c \equiv b + d, \quad a \cdot c \equiv b \cdot d, \quad -a \equiv -b \pmod{m}$$

In altre parole, ogni qualvolta in una congruenza abbiamo una somma, una sottrazione o un prodotto, possiamo sostituire i termini che lo compongono con altri termini che ci rendono più facili i calcoli, a patto che questi abbiano lo stesso resto modulo m .

Per esempio, per calcolare $(324 \cdot 231) \pmod{10}$ non è necessario svolgere effettivamente il prodotto, ma si possono sostituire i fattori con i termini equivalenti $4 \equiv 324 \pmod{10}$ e $1 \equiv 231 \pmod{10}$, ottenendo immediatamente il risultato $4 \cdot 1 = 4$.

Notare che queste proprietà si applicano anche nel caso dell'elevamento a potenza fissato l'esponente, essendo esso una moltiplicazione ripetuta:

$$a \equiv b \pmod{m} \implies a^n \equiv b^n \pmod{m}$$

Calcolare $4931^{4931} \pmod{9}$.

Possiamo sfruttare il fatto che $4931 \pmod{9} = (4 + 9 + 3 + 1) \pmod{9} = 8$, e che quindi $4931 \equiv 8 \equiv -1 \pmod{9}$, per cui $4931^{4931} \pmod{9} = (-1)^{4931} \pmod{9} = -1 \pmod{9} = 8$. Notare che questo metodo ci consente di ridurre la base a valori più comodi, ma non ugualmente l'esponente che non può essere sostituito. Siamo stati quindi fortunati a trovare proprio il resto -1 , del quale è semplice calcolare le potenze anche molto grandi. Altrimenti avremmo dovuto ricorrere a ragionamenti leggermente più sofisticati (cfr. 2.2.4).

2.2.3 Divisione e semplificazione

Anche se tra i numeri interi è noto che non sempre esistono i reciproci (cioè i numeri del tipo $\frac{1}{a}$), all'interno delle congruenze è possibile definirli in modo del tutto analogo a quanto avviene nei numeri razionali. Dati a e m interi si dice quindi *inverso* di a (modulo m) quel numero $a^{-1} = b$ tale per cui $a \cdot b \equiv 1 \pmod{m}$. Non sempre l'inverso esiste, ma se esiste è certamente unico.

Per esempio, modulo 7 abbiamo che $2^{-1} = 4$ e $3^{-1} = 5$, infatti $2 \cdot 4 = 8 \equiv 1 \pmod{7}$, $3 \cdot 5 = 15 \equiv 1 \pmod{7}$. Nella maggior parte dei casi, il miglior modo di trovare l'inverso è procedere per tentativi.

È facile verificare che l'inverso esiste se e solo se il $MCD(a, m) = 1$. Infatti $a \cdot b \equiv 1 \pmod{m} \implies a \cdot b = 1 + k \cdot m \implies a \cdot b - k \cdot m = 1$, e per il Teorema di Bezout il primo membro è sempre multiplo di $MCD(a, m)$ al variare di b e k .

In modo del tutto analogo si comporta la semplificazione. Infatti in una congruenza del tipo $a \cdot c \equiv b \cdot c \pmod{m}$ si può semplificare per c e ottenere $a \equiv b \pmod{m}$ solo se $MCD(c, m) = 1$; risultato che si ottiene semplicemente moltiplicando i due membri per l'inverso di c .

In caso contrario, è comunque possibile una semplificazione, facendo attenzione a dividere però anche il modulo:

$$a \cdot c \equiv b \cdot c \pmod{m \cdot c} \implies a \equiv b \pmod{m}$$

Riformulare l'espressione $2 \cdot 4 \equiv 5 \cdot 4 \pmod{6}$.

Sebbene questa espressione sia certamente vera, se semplifichiamo per 4 otteniamo la relazione scorretta $2 \equiv 5 \pmod{6}$. Possiamo però dividere tutto per 2, compreso il modulo, ottenendo $2 \cdot 2 \equiv 5 \cdot 2 \pmod{3}$ e poi semplificare per il 2 rimanente e ottenere la relazione corretta $2 \equiv 5 \pmod{3}$.

2.2.4 Operazioni ripetute

Uno dei punti di forza delle congruenze è la facilità con la quale vengono calcolate le operazioni ripetute. Essendo infatti possibili soltanto m valori distinti, entro al più m passaggi si troverà un valore che è già comparso precedentemente. Da quel punto in poi, tutti i valori che si troveranno si ripeteranno ciclicamente tra quelli già trovati (infatti applicando l'operazione allo stesso numero si ottiene lo stesso risultato). In pratica, se iterando un'operazione i risultati si ripetono ogni k passi, allora possiamo ridurre il numero di volte in cui questa viene ripetuta facendo $n \bmod k$ e considerando il risultato ottenuto.

Calcolare $2^{546321} \bmod 12$.

Calcolare una potenza di 2 equivale a ripetere la moltiplicazione per 2 partendo da 1. Modulo 12 otterremo quindi la sequenza 1, 2, 4, 8, 4, ... Avendo ora trovato un elemento ripetuto (il 4), sappiamo che d'ora innanzi la sequenza proseguirà alternando il 4 e l'8, come si può facilmente verificare. Dato poi che i risultati si ripetono ogni 2 passi, e $546321 \bmod 2 = 1$, immediatamente si ottiene che il valore cercato è 8.

2.2.5 Residui quadratici

Si dicono residui quadratici (o in generale n -esimi) modulo m tutte le possibili classi di resto che possono assumere i quadrati perfetti (o in generale le n -esime potenze) modulo m . Se si escludono i casi $m \leq 2$, non tutte le classi di resto sono possibili; per cui con questa tecnica in un'equazione a valori interi spesso si riescono ad escludere alcuni casi ed è possibile così avvicinarsi alla soluzione. Per esempio, modulo 4 abbiamo che $0^2 = 0$; $1^2 = 1$; $2^2 = 4 \equiv 0$; $3^2 = 9 \equiv 1$, quindi i soli resti possibili per le potenze sono effettivamente 0 e 1. Vediamo ora alcuni esempi:

- I residui quadratici modulo 3 sono [0] e [1].
- I residui quadratici modulo 4 sono [0] e [1]. In particolare, il quadrato di un intero pari è congruo a 0, e quello di un intero dispari è congruo a 1.
- I residui quadratici modulo 5 sono [0], [1] e $[-1] = [4]$.

- I residui quadratici modulo 8 sono $[0]$, $[1]$ e $[4]$.
- I residui terzi modulo 7 sono $[0]$, $[1]$ e $[-1] = [6]$.
- I residui quarti modulo 16 sono $[0]$ e $[1]$.
- I residui quinti modulo 11 sono $[0]$, $[1]$ e $[-1] = [10]$.

È possibile estendere la lista ad altri casi che sono di interesse, semplicemente provando a svolgere i calcoli su tutti i possibili resti da 0 a $m - 1$.

2.2.6 Sistemi di congruenze

Un sistema di congruenze, analogamente a un sistema di equazioni, è dato da un certo numero di congruenze con la richiesta che siano tutte soddisfatte. Il risultato fondamentale che consente di risolverli è che ogni sistema di congruenze o è impossibile, o è equivalente a una singola congruenza, con modulo dato dal minimo comune multiplo di tutti i moduli. Sapendo questo, risulta possibile passare a risolverli per tentativi.

Alberto, Beppe e Carlo vogliono trovarsi dopo il capodanno una sera per rievocare i bei vecchi tempi. Alberto ha una serata libera ogni 6 giorni a partire dal 2 di Gennaio, Beppe ha invece una sola serata libera ogni 15 giorni a partire dall'11, e Carlo ne ha una libera ogni 8 giorni a partire dal 5. Quando riusciranno a incontrarsi tutti e tre? E se invece Alberto e Beppe vogliono incontrarsi da soli?

Schematizziamo le sere libere con il seguente sistema di equazioni:

$$\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 11 \pmod{15} \\ x \equiv 5 \pmod{8} \end{cases}$$

Questo sistema è impossibile, infatti la prima equazione richiede che x sia pari, mentre la terza equazione richiede che x sia dispari, pertanto i tre amici non si potranno mai trovare insieme. Proviamo allora a risolvere il sistema formato dalle sole prime due equazioni, considerando quindi solo Alberto e Beppe. Certamente questo è equivalente a una congruenza modulo $30 = \text{mcm}(6, 15)$, e quindi ha una soluzione compresa tra 0 e 29. Allora procedendo per tentativi possiamo elencare le soluzioni della seconda equazione (che avendo un modulo più grande ne ha meno) fino a 30, ottenendo 11 e 26. La soluzione $x \equiv 26 \pmod{30}$ soddisfa anche la prima equazione, quindi Alberto e Beppe potranno trovarsi ogni 30 giorni a partire dal 26 di Gennaio.

L'equivalenza tra singole congruenze e sistemi è a volte utile anche nel verso contrario. Se infatti abbiamo la congruenza $x \equiv a \pmod{m = m_1 \cdot m_2 \cdot \dots \cdot m_k}$, con gli m_1, \dots, m_k tutti relativamente primi tra loro, possiamo equivalentemente sostituirla con il sistema $x \equiv a \pmod{m_i}$ con $i = 1 \dots k$. Questo risulta solitamente utile prendendo come moduli m_i i fattori primi $p_i^{\alpha_i}$ di m .

Come strategia generale per risolvere un sistema, spesso è utile prima dividere ogni congruenza secondo i fattori primi di m come descritto sopra, poi raggruppare tutte quelle relative allo stesso numero primo e verificarne la compatibilità con la congruenza con esponente α_i più grande. In caso affermativo, si passa a risolvere il sistema trascurando le ridondanze, cioè conservando per ogni primo solo la congruenza con esponente più grande.

Risolvere il problema precedente, sfruttando questo fatto.

Rielaboriamo il precedente sistema di equazioni:

$$\left\{ \begin{array}{l} x \equiv 2 \pmod{6} \\ x \equiv 11 \pmod{15} \\ x \equiv 5 \pmod{8} \end{array} \right. \implies \left\{ \begin{array}{l} x \equiv 2 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 11 \pmod{3} \\ x \equiv 11 \pmod{5} \\ x \equiv 5 \pmod{8} \end{array} \right. \implies \left\{ \begin{array}{l} x \equiv 5 \pmod{8} \\ x \equiv 2 \pmod{2} \\ x \equiv 11 \pmod{3} \\ x \equiv 2 \pmod{3} \\ x \equiv 11 \pmod{5} \end{array} \right.$$

In questo modo ci si accorge immediatamente che il sistema è impossibile sostituendo la prima nella seconda ($5 \not\equiv 2 \pmod{2}$). Se come prima poi trascuriamo la terza equazione originaria, ed eliminiamo la ridondanza delle due congruenze modulo 3, abbiamo il sistema:

$$\left\{ \begin{array}{l} x \equiv 0 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \end{array} \right.$$

Che si può passare poi a risolvere ottenendo nuovamente $x \equiv 26 \pmod{30}$.

2.2.7 Uso delle congruenze

L'utilità delle congruenze risiede nella relativa semplicità con cui si possono fare quasi ogni tipo di conti. Tuttavia, solo in alcuni casi questo è utile, poiché conoscere il valore di un'espressione modulo m dà certamente molte meno informazioni che conoscerne l'effettivo valore. In almeno due tipi di problemi però le congruenze sono effettivamente efficaci. Un primo tipo di problemi richiede l'applicazione pura e semplice delle congruenze, solitamente mascherata tramite alcuni stratagemmi. Per esempio:

- Trovare la cifra delle unità di una certa espressione, o le due cifre più a destra, o simili, significa in realtà calcolare il valore dell'espressione data modulo 10, o 100, o altre potenze di 10.
- Similmente, problemi che riguardano la somma delle cifre di un numero o la somma alternata si rifanno ai criteri di congruenza per 9 e 11, e quindi potrebbero far buon uso delle congruenze.
- Alcuni problemi, infine, riguardano la divisibilità di un numero per un altro, e possono efficacemente essere schematizzati con una relazione del tipo $x \equiv 0 \pmod{d}$.

Un secondo tipo, forse più interessante, è dato invece da problemi che richiedono di trovare soluzioni intere di alcune equazioni. Anche se le congruenze non possono mai dare la certez-

za dell'esistenza di soluzioni, si rivelano preziose per eliminare classi di interi dalle soluzioni possibili, semplificando così il problema e restringendolo a possibilità su cui è più semplice ragionare.

2.3 Equazioni Diofantee

Un'equazione Diofantea è un'equazione numerica qualunque della quale si richiedono le soluzioni intere, affiancata eventualmente da condizioni aggiuntive sulle variabili: per esempio, che una certa variabile p sia un numero primo. Di solito un'equazione Diofantea ha un certo numero di soluzioni semplici che possono essere trovate per tentativi; una volta trovate queste normalmente occorre dimostrare che non ce ne sono altre. Altre volte può capitare che un'equazione Diofantea abbia come soluzioni un'intera classe di numeri.

2.3.1 Equazioni diofantee di primo grado in due variabili

Un'equazione Diofantea di primo grado in due variabili è un'espressione di questo tipo:

$$ax + by = c$$

dove a, b, c sono dati e x, y sono le incognite. Se $MCD(a, b)$ non è divisore di c , l'equazione non ha soluzioni. In caso contrario, ne ha infinite. Per ottenerle, è possibile utilizzare il *metodo delle divisioni iterate di Euclide*, basato sull'algoritmo di Euclide per l'MCD.

Trovare le soluzioni intere per l'equazione:

$$86x + 25y = 1$$

Siccome $a = 86 = 2 \cdot 43$; $b = 25 = 5^2$ si ha che $MCD(86, 25) = 1$, che è un divisore di $c = 1$. Quindi ci sono infinite soluzioni. Si usano le divisioni con resto iterate:

$$86 = 3 \cdot 25 + 11$$

$$25 = 2 \cdot 11 + 3$$

$$11 = 3 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

Nel primo passaggio, il dividendo è a e il divisore è b . In ciascuno dei passaggi successivi, come nuovo dividendo si prende il divisore della riga precedente, e come nuovo divisore si prende il resto della riga precedente. Ci si ferma quando l'ultimo resto ottenuto è $MCD(a, b)$. Si possono ora trovare x e y , riscrivendo l'ultima divisione e compiendo i

seguenti passaggi, in cui si sostituiscono i resti ottenuti sopra, in ordine inverso:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 = \\ &= 3 - 1 \cdot (11 - 3 \cdot 3) = 4 \cdot 3 - 1 \cdot 11 = \\ &= 4 \cdot (25 - 2 \cdot 11) - 1 \cdot 11 = 4 \cdot 25 - 9 \cdot 11 = \\ &= 4 \cdot 25 - 9 \cdot (86 - 3 \cdot 25) = -9 \cdot 86 + 31 \cdot 25 \end{aligned}$$

I resti ottenuti sopra in ordine inverso sono 1,2,3,11. In ogni nuova riga, il passaggio consiste nel sostituire il resto, indicato in neretto, con l'espressione in parentesi, che si ricava dalle quattro divisioni di prima. Ad esempio, nella terza riga **3** viene sostituito con $(25 - 2 \cdot 11)$, ottenuto dalla seconda divisione: $25 = 2 \cdot 11 + 3$. Poi la parentesi viene sciolta e si continua con la riga seguente, sostituendo il prossimo resto. Alla fine, si ottiene $1 = -9 \cdot 86 + 31 \cdot 25$, e quindi $x = -9$ e $y = 31$. Da questa soluzione, si trovano facilmente tutte le altre, che sono $x = -9 + 25k$ e $y = 31 - 86k$, dove k è un qualsiasi intero.

Il metodo usato è applicabile in tutti i casi in cui esistono soluzioni. Se a, b, c all'inizio non sono coprimi, naturalmente si riduce l'equazione: ad esempio $258x + 75y = 3$ si trasforma in $86x + 25y = 1$ dividendo ogni termine per 3; se $c \neq 1$, come nel caso $86x + 25y = 7$, si adatta la soluzione di $86x + 25y = 1$ moltiplicandola per 7: $x = -63$ e $y = 217$. Invece, nel caso di $42x + 30y = 16$, dopo averla ridotta in $21x + 15y = 8$ dividendo ogni termine per 2, si nota che $MCD(21, 15) = 3$ non divide 8 e quindi l'equazione non ha nessuna soluzione.

Soluzione problema di inizio capitolo.

Il problema di inizio capitolo si può formulare in termini di equazioni diofantee: infatti, sia x il numero iniziale di noci di cocco. Dopo che il primo marinaio si appropria (indebitamente) di alcune di esse, in totale ne rimangono $\{\frac{4}{5}(x-1)\}$. Si noti che per i dati che abbiamo, tale quantità è un numero intero. Dopo le attività notturne del secondo marinaio le noci di cocco si riducono a $\{\frac{4}{5}(\frac{4}{5}(x-1)-1)-1\}$. Ripetendo questo ragionamento, si ha che al mattino restano $\{\frac{4^5}{5^5}x - \frac{8404}{3125}\}$ noci di cocco. Togliendone una per la scimmia abbiamo che $\{\frac{4^5}{5^5}x - \frac{11529}{3125}\}$ è un numero intero divisibile per 5: se lo chiamiamo $5y$ trovato che il minimo x intero che soddisfa l'equazione diofantea $\{\frac{4^5}{5^5}x - \frac{11529}{3125} = 5y\}$ è la soluzione al problema. Facendo i calcoli mediante l'algoritmo di Euclide troviamo che è 15621.

2.3.2 Metodo di scomposizione parziale

Un primo metodo per restringere il campo delle possibili soluzioni in un'equazione Diofantea è quello della fattorizzazione numerica. Innanzitutto occorre portare l'equazione tutta al

primo membro, ottenendo una scrittura quindi del tipo $f(x) = 0$. Se già sappiamo scomporre $f(x)$ è facile trovare le soluzioni; altrimenti cerchiamo una costante k opportuna che, aggiunta a $f(x)$, ci consenta di scomporlo. In formule, si cerca di trovare un k tale per cui sappiamo scomporre $f(x) + k = g(x) \cdot h(x)$. Ricavati quindi $g(x)$ e $h(x)$, potremo riscrivere l'equazione iniziale come $k = f(x) + k = g(x) \cdot h(x)$; ma poiché le due espressioni $h(x)$ e $g(x)$ assumono solo valori interi, le possibilità di ottenere k come prodotto di interi non sono infinite. Se infatti esaminiamo i fattori primi di k , distribuendoli in tutti i modi possibili tra il primo e il secondo fattore, ci ricondurremo a un certo numero di sistemi di due equazioni del tipo $g(x) = d_1$, $h(x) = d_2$ (con $d_1 \cdot d_2 = k$) normalmente molto più semplici da risolvere, che esauriscono tutti i casi. Questo procedimento richiede che la scomposizione sia fatta solo all'interno dei numeri interi, ma è possibile generalizzarlo a scomposizioni razionali (moltiplicando i due membri di $k = g(x) \cdot h(x)$ per il minimo comune denominatore di $g(x)$ e $h(x)$).

Trovare le soluzioni intere positive dell'equazione:

$$xy + x = 2007y + 2$$

Così com'è, non è possibile scomporre questo polinomio. Se però portiamo tutto al primo membro e proviamo a togliere 2005 a entrambi i membri otteniamo

$$xy + x - 2007y - 2005 - 2 = -2005 \Leftrightarrow (x - 2007) \cdot (y + 1) = -2005$$

Ma poiché cerchiamo soluzioni intere positive, certamente $y + 1 \geq 2$, allora il fattore negativo dev'essere $x - 2007 < 0$. Inoltre scomponiamo $2005 = 5 \cdot 401$, e proviamone tutti i possibili divisori sul secondo fattore:

- $y + 1 = 1 \Leftrightarrow y = 0$: Impossibile, perché chiedevamo y intero positivo
- $y + 1 = 5 \Leftrightarrow y = 4, x - 2007 = -401 \Leftrightarrow x = 1606$: Prima soluzione
- $y + 1 = 401 \Leftrightarrow y = 400, x - 2007 = -5 \Leftrightarrow x = 2002$: Seconda soluzione
- $y + 1 = 2005 \Leftrightarrow y = 2004, x - 2007 = -1 \Leftrightarrow x = 2006$: Terza soluzione

L'equazione è quindi risolta, e le tre soluzioni sono $(1606, 4), (2002, 400), (2006, 2004)$.

2.3.3 Metodo delle congruenze

Il altro metodo spesso utilizzato per dimostrare che un'equazione Diofantea non ha soluzioni (magari dopo aver posto condizioni aggiuntive sulle variabili per escludere le soluzioni già trovate), è valutarne la congruenza modulo un qualche m , e dedurre che la relativa congruenza è impossibile. Se lo è, lo sarà anche l'equazione originale (numeri uguali hanno lo stesso resto modulo m qualunque). Per meglio visualizzare l'aiuto fornito dalle condizioni, se per esempio

si ricava che la variabile p numero primo deve essere $p \equiv 0 \pmod{3}$, allora si può dedurre che proprio $p = 3$; e sostituendo direttamente nell'equazione si verifica se effettivamente questa individua una soluzione.

Quali sono le coppie (p, n) di interi non negativi con p primo tali che $p^2 + n - 3 = 6^n + n^6$?

L'equazione $p^2 + n - 3 = 6^n + n^6$ comprende due termini, -3 e 6^n , che sparirebbero considerandola modulo 3. Prima si deve prestare attenzione al caso particolare $n = 0$, un valore accettabile in quanto non negativo. Solo in questo caso $6^n = 6^0 = 1$ e quindi 6^n non è congruente a 0 modulo 3. Sostituendo $n = 0$ si ottiene $p^2 - 3 = 1$ e quindi la soluzione accettabile $(2, 0)$.

Se invece $n \neq 0$, si considera l'equazione di partenza modulo 3: $p^2 + n \equiv n^6$ cioè $p^2 \equiv n^6 - n$. Si analizzano i tre casi $n \equiv 0, 1, 2 \pmod{3}$: se $n \equiv 0$ allora $p^2 \equiv 0^6 - 0 = 0$; se $n \equiv 1$ allora $p^2 \equiv 1^6 - 1 = 0$; $n \equiv 2$ allora $p^2 \equiv 2^6 - 2 = 64 - 2 = 62 \equiv 2$. Il terzo caso è impossibile: infatti, un quadrato perfetto non è mai congruo a 2 modulo 3; detto in altre parole, 2 non è un residuo quadratico modulo 3. Segue che, in ogni caso, $p^2 \equiv 0 \pmod{3}$. Questo significa che, ricordando la definizione stessa di congruenza, $3 \mid p^2$, e quindi $3 \mid p$. Siccome p è un numero primo, l'unica possibilità è $p = 3$. Si sostituisce questo valore nell'equazione di partenza, ricavando $9 + n - 3 = 6^n + n^6$ cioè $6 + n = 6^n + n^6$. Secondo il testo del problema, n deve essere non negativo, e il caso $n = 0$ è stato già trattato. Quindi $n \geq 1$, il che determina $6^n \geq 6$ e $n^6 \geq n$, con uguaglianza nel solo caso $n = 1$. Segue che $6^n + n^6 \geq 6 + n$ e l'uguaglianza vale se e solo se $n = 1$. In questo modo si determina la seconda soluzione $(3, 1)$, e si prova anche che non ne esistono altre.

Trovare le soluzioni intere, se ce ne sono, per l'equazione:

$$42^a + a^{42} = 26^a \cdot a^{26}$$

Tentare di risolvere esplicitamente l'equazione data è impensabile, ma se esiste un a che la soddisfa, lo stesso soddisferà anche $42^a + a^{42} \equiv 26^a \cdot a^{26} \pmod{5}$. Questa è molto più facile da risolvere, e tenendo presente che $42 \equiv 2, 26 \equiv 1 \pmod{5}$ l'equazione può essere riscritta come $2^a + a^{42} \equiv 1^a \cdot a^{26} \equiv a^{26} \pmod{5}$. Si verifica poi che modulo 5 tutte le potenze si ripetono ciclicamente ogni 4 volte, cioè $a^5 = a$ per ogni a ($0^5 = 0, 1^5 = 1, 2^5 = 32 \equiv 2, 3^5 \equiv (-2)^5 = -(2^5) \equiv -2 \equiv 3, 4^5 \equiv (-1)^5 = -1 \equiv 4$). Dato poi che $42 \equiv 2, 26 \equiv 1 \pmod{4}$, allora anche $a^{42} = a^{40} \cdot a^2 = (a^4)^{10} \cdot a^2 \equiv 1^{10} \cdot a^2 = a^2$ e allo stesso modo $a^{26} \equiv a^2$. Possiamo allora scrivere $2^a + a^2 \equiv a^2 \pmod{5} \implies 2^a \equiv 0 \pmod{5}$. Ma questo è chiaramente impossibile, e quindi anche l'equazione iniziale non ha soluzioni.

2.4 Approfondimenti

2.4.1 Elevamento a potenza

Abbiamo accennato prima alla strategia per tentativi nel caso di operazioni ripetute. Tuttavia, almeno nel caso delle potenze, esiste un metodo per calcolarne esattamente e velocemente le classi di congruenza. Cerchiamo di arrivarci partendo dal metodo per tentativi.

Trovare la cifra delle unità di 2007^{2007} .

La cifra delle unità significa la sua congruenza modulo 10. Sappiamo già che è possibile ridurre la base: siccome $2007 \equiv 7$, allora $2007^{2007} \equiv 7^{2007} \pmod{10}$. Per ridurre l'esponente, procediamo per tentativi come abbiamo visto, elencando le prime potenze di 7 modulo 10:

$$7^0 \equiv 1, \quad 7^1 \equiv 7, \quad 7^2 \equiv 49 \equiv 9, \quad 7^3 = 7^2 \cdot 7 \equiv 9 \cdot 7 \equiv 63 \equiv 3, \quad 7^4 \equiv 21 \equiv 1$$

Siccome l'ultimo risultato è uguale al primo, e il calcolo di ogni valore dipende solo dal precedente, le potenze saranno periodiche da questo punto in poi, ovvero si otterranno gli stessi resti nello stesso ordine. In altre parole, $7^1, 7^2, 7^3, 7^4, 7^5, 7^6, 7^7, 7^8, 7^9, \dots$ sono congruenti modulo 10 a $7, 9, 3, 1, 7, 9, 3, 1, 7, \dots$ rispettivamente. Quindi nel caso che stiamo trattando l'esponente si ripete ogni 4, ovvero si riduce modulo 4: preso un numero naturale a , 7^a è congruo modulo 10 a $1, 7, 9, 3$ rispettivamente nei casi $a \equiv 0, 1, 2, 3 \pmod{4}$, e quindi $7^a \equiv 7^{a \bmod 4} \pmod{10}$.

2007 è congruente modulo 4 alle sue ultime due cifre, quindi $2007 \equiv 7 \equiv 3 \pmod{4}$. Segue che $2007^{2007} \equiv 7^{2007} \equiv 7^3 \equiv 3 \pmod{10}$. La cifra delle unità di 2007^{2007} quindi è 3.

Tutti i passaggi appena effettuati possono essere considerati come un'applicazione delle proprietà delle potenze: $7^{2007} = 7^{4 \cdot 501 + 3} = 7^{4 \cdot 501} \cdot 7^3 = (7^4)^{501} \cdot 7^3 \equiv 1^{501} \cdot 3 = 3 \pmod{10}$. Il calcolo delle potenze si riesce quindi a semplificare, riducendo anche l'esponente, se si riesce a trovare ogni quanto tempo le potenze si ripetono come prima abbiamo fatto per tentativi; e le potenze dovranno per forza ripetersi da un certo punto in poi dato che i valori che possono assumere sono finiti (da 0 a $m - 1$ se stiamo considerando resti modulo m).

Il periodo con il quale si ripetono le potenze di un numero, 4 nell'esempio precedente, si chiama *ordine moltiplicativo* di 7 modulo 10: in generale dato un a con $\text{MCD}(a, m) = 1$, si chiama ordine moltiplicativo di a modulo m , e si scrive $\text{ord}_a(m)$, il più piccolo intero positivo tale che $a^n \equiv 1 \pmod{m}$.

Inoltre definiamo $\text{ord}(m)$ il massimo degli ordini moltiplicativi $\text{ord}_a(m)$ al variare di a . Per fortuna, il valore $\text{ord}(m)$ si riesce a calcolare facilmente ed è anche possibile utilizzarlo al posto di $\text{ord}_a(m)$.

Infatti vale sempre, per ogni a , che:

$$\text{ord}_a(m) \mid \text{ord}(m)$$

Il che si traduce nel fatto che:

$$a^{\text{ord}(m)} = a^{k \cdot \text{ord}_a(m)} = (a^{\text{ord}_a(m)})^k \equiv 1^k \equiv 1 \pmod{m}$$

Quindi l'ordine moltiplicativo è proprio il modulo con il quale ridurre l'esponente.

L'ordine moltiplicativo, nel caso di un modulo $m = p^k$ potenza di un primo, è il massimo che ci si potrebbe aspettare: cioè è pari al numero di elementi non multipli di p fino a p^k (è evidente che un a non multiplo di p non può diventarne multiplo facendo delle potenze). I multipli di p sono uno

ogni p , quindi in formule avremo:

$$\text{ord}(p^k) = p^k - \frac{1}{p}p^k = p^k - p^{k-1}$$

A questo punto passare al caso generale è questione di un attimo, infatti (per il discorso fatto sui sistemi di congruenze) avere una congruenza modulo $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots$ equivale ad avere una congruenza per ogni $p_i^{\alpha_i}$, ciascuna delle quali si ripete ogni $\text{ord}(p_i^{\alpha_i})$. Il sistema totale si ripeterà ogni volta che si sono ripetute tutte le sue equazioni, e quindi sarà il minimo comune multiplo del periodo di ciascuna:

$$\text{ord}(p_1^{\alpha_1} p_2^{\alpha_2} \dots) = \text{mcm}(\text{ord}(p_1^{\alpha_1}), \text{ord}(p_2^{\alpha_2}), \dots)$$

Riassumendo, per calcolare il modulo di una potenza $a^b \bmod m$ bisogna fare:

$$(a \bmod m)^{b \bmod \text{ord}(m)} \pmod{m}$$

E scomponendo in fattori $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots$ avremo che:

$$\text{ord}(m) = \text{mcm}(p_1^{\alpha_1} - p_1^{\alpha_1-1}, p_2^{\alpha_2} - p_2^{\alpha_2-1}, \dots)$$

Calcolare le ultime due cifre di $2007^{2007^{2007}}$.

Dobbiamo calcolare $2007^{2007^{2007}} \bmod 100$, quindi per quanto visto prima basta fare:

$$(2007 \bmod 100)^{2007^{2007} \bmod \text{ord}(100)} \pmod{100}$$

Dato che $\text{ord}(100) = \text{ord}(2^2 \cdot 5^2) = \text{mcm}(2^2 - 2^1, 5^2 - 5^1) = \text{mcm}(2, 20) = 20$, e $2007 \bmod 100 = 7$, ci resta solo più da calcolare $2007^{2007} \bmod 20$. Riapplichiamo lo stesso ragionamento:

$$2007^{2007} \bmod 20 = (2007 \bmod 20)^{2007 \bmod \text{ord}(20)} \pmod{20}$$

Dato che $\text{ord}(20) = \text{ord}(2^2 \cdot 5^1) = \text{mcm}(2^2 - 2^1, 5^1 - 5^0) = \text{mcm}(2, 4) = 4$, avremo finalmente:

$$2007^{2007^{2007}} \bmod 100 = (2007 \bmod 100)^{(2007 \bmod 20)^{2007 \bmod 4}} \pmod{100}$$

calcolando i moduli:

$$= 7^{7^3=49 \cdot 7=9 \cdot 7=63 \equiv 3} \pmod{100}$$

$$= 7^3 = 343 \equiv 43 \pmod{100}$$

La risposta quindi è 43.

2.5 Esercizi

2.5.1 Esercizi di base

Operazioni e relazioni fondamentali

1. a) Calcolare $3249 \operatorname{div} 2$, $2384 \operatorname{div} 5$, $66 \operatorname{div} 7$, $947 \operatorname{div} 9$.
 - b) Calcolare $2618259 \operatorname{mod} n$ per:

$n = 2$	$n = 3$	$n = 4$	$n = 5$
$n = 7$	$n = 8$	$n = 9$	$n = 10$
$n = 11$	$n = 16$	$n = 25$	$n = 100$
 - c) Sfruttando i risultati al punto precedente, calcolare il modulo con:

$n = 6$	$n = 15$	$n = 21$	$n = 22$
$n = 75$	$n = 900$	$n = 6300$	$n = 2618200$
 - d) Calcolare $3698 \cdot 7773 \operatorname{mod} 9$, $35461^{54593428} \operatorname{mod} 11$, $(353094232 \operatorname{mod} 721) \operatorname{mod} 9$
 - e) Calcolare $\operatorname{MCD}(4539, 6284)$, $\operatorname{mcm}(4539, 6284)$.
2. a) Trovare un esempio di numero divisibile per n con:

$n = 2$	$n = 3$	$n = 4$	$n = 5$
$n = 6$	$n = 8$	$n = 9$	$n = 10$
$n = 11$	$n = 12$	$n = 15$	$n = 16$
$n = 33$	$n = 36$	$n = 100$	$n = 125$

 - b) Scrivere un numero di 5 cifre divisibile per i precedenti n .
 - c) Prese le 10 cifre, scrivere un numero di 10 cifre (tutte diverse) in modo che sia divisibile per i precedenti n .
 - d) Prova che sommando (o sottraendo) due numeri divisibili per n , si ottiene un numero a sua volta divisibile per n .

Congruenze

3. Trova tutti i numeri tali che:

$$x \equiv 2 \pmod{7} \quad x \equiv 4 \pmod{8} \quad 7x \equiv 2 \pmod{8}$$

$$2x \equiv 1 \pmod{4} \quad \begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 4 \pmod{8} \end{cases} \quad \begin{cases} 7x \equiv 2 \pmod{8} \\ 2x \equiv 1 \pmod{4} \end{cases}$$

4. a) Compila la seguente tabella:

x^2	mod 2	mod 3	mod 4	mod 5	mod 6	mod 7	mod 8	mod 9
1								
4								
9								
16								
25								
36								
49								
64								
81								
100								
121								
144								
169								

b) Dire quali di questi numeri (scritti nella forma $ak + b$) possono essere dei quadrati perfetti per opportuni k :

$$\begin{array}{lll} 3k+2 & 5k+2 & 7k+3 \\ 4k+2 & 6k+2 & 7k-2 \\ 4k-1 & 6k+5 & 7k-1 \end{array}$$

c) Trova tutti i valori di k per cui i seguenti numeri sono quadrati perfetti:

$$7k+3 \quad 6k+2 \quad 28k^3+24k^2+3k-1$$

2.5.2 Esercizi svolti

1. Un canguro sale una scala di 5000 gradini saltando prima sul 3°, poi scendendo di 1, salendo di 5, scendendo di 3, salendo di 7 e così via. Purtroppo uno scalino è pericolante. Il canguro potrà salire la scala solo se lo scalino pericolante è:
 (A) il 2000° (B) il 2001° (C) il 2002° (D) il 2003°
 (E) Cadrà comunque

2. Sia x la somma degli interi dispari da 1 a $2k+1$. Quali di questi valori non può assumere x ?
 (A) 625 (B) 1225 (C) 2025 (D) 3025 (E) 4525

3. La cifra delle unità del numero 2137^{753} è:
 (A) 1 (B) 3 (C) 5 (D) 7 (E) 9

4. Il numero n diviso per 1995 dà resto 29, inoltre n dà resto 29 anche se diviso per 1996. Qual è l'ultima cifra di n ?
 (A) 5 (B) 3 (C) 4 (D) 7 (E) 9

5. Per quali valori di n , l'espressione $n^2 - 14n + 24$ è un numero primo?
6. Quali interi risolvono l'equazione $(x^2 - x - 1)^{x+2} = 1$?
7. Per quali coppie (a, b) di naturali si ha $a^2 - 4b^2 = 45$?
8. Se n è un intero positivo, quale fra i seguenti è certamente divisibile per 3?
 (A) $(n+2)(n+3)(n+5)$ (B) $n(n+2)(n+6)$ (C) $n(n+2)(n+4)$
 (D) $n(n+3)(n-3)$ (E) $(n+1)(n+2)$
9. I numeri a, b sono interi positivi. Qual è il minimo valore positivo di $a + b$ affinché $21ab^2$ e $15ab$ siano entrambi quadrati perfetti?
 (A) 16 (B) 26 (C) 36 (D) 46 (E) 56
10. Quante sono le progressioni aritmetiche costituite da quattro numeri interi a, b, c, d con $1 \leq a < b < c < d \leq 100$?

2.5.3 Esercizi proposti

1. Quanto vale la somma delle cifre di $(999.999.999.999.995)^2$?
2. Quanto vale la cifra delle unità di $3^{3^{\dots^3}}$, dove compaiono ben cento 3?
3. Si consideri l'equazione:
- $$x^{2007} = y^x$$
- a) Determinare tutte le soluzioni (x, y) con x intero primo e y intero positivo.
 b) Determinare tutte le soluzioni (x, y) con x e y interi positivi.
4. Trovare tutte le soluzioni intere dell'equazione $x^2 + y^2 + z^2 = 2xyz$.
5. Quante coppie ordinate positive (x, y) soddisfano l'equazione $xy + 5(x + y) = 2005$?
6. Quali sono le coppie di interi primi (p, q) che verificano l'equazione $p^2 + pq + 275p + 10q = 2008$?
7. Quante sono le coppie di interi positivi (x, y) che verificano l'equazione $x^2 + y^2 - 2004x - 2004y + 2xy - 2005 = 0$?
8. Determinare tutte le terne (m, n, p) tali che $p^n + 144 = m^2$, dove m e n sono interi positivi e p è intero primo.
9. Si dica per quanti valori di n il numero $n^2 + 340$ è un quadrato.
10. Un numero è composto da 77 cifre, tutte uguali a 7. Qual è il resto della divisione di questo numero per 101?

11. Alberto deve a Barbara 11 euro. Essi sono entrambi allevatori, e non avendo monete nè banconote, hanno stabilito che una mucca vale 30 euro e una pecora ne vale 17. Qual'è il numero minimo di animali che devono passare di proprietà affinché Alberto possa ripagare Barbara? (Se ad esempio Alberto dovesse pagare 13 euro, potrebbe cedere una mucca a Barbara e ricevere una pecora di resto).
12. Sia n il più piccolo intero positivo > 200 che si può scrivere sia come somma di 5 interi consecutivi, sia come somma di 6 interi consecutivi, sia come somma di 7 interi consecutivi. Quanto vale n ?
13. Sia data una progressione aritmetica infinita di numeri naturali. Si dica se le seguenti affermazioni sono corrette, giustificando la risposta.
 - Se 3 divide un termine della progressione allora vi è un termine divisibile per 9.
 - Se c'è un termine divisibile per 3, allora ce ne sono infiniti.
 - Se 2 divide un termine della progressione e 3 divide un altro termine, allora vi è un termine divisibile per 6.
14. Dalle passate olimpiadi[3]: ARIT61, ARIT67, ARIT71, ARIT74, ARIT83, ARIT87, ARIT88, ARIT89, ARIT94, ARIT101, ARIT102, ARIT104, ARIT106, ARIT107, ARIT108, ARIT114, ARIT115, ARIT116, ARIT119, ARIT122, ARIT125.

L'*algebra*, nella classificazione dei problemi olimpici, si occupa in generale dello studio delle proprietà dei numeri razionali, reali e complessi; ma gli argomenti principali trattati sono in realtà lo studio di polinomi, successioni, disuguaglianze e funzioni.

Siano a, b, c le soluzioni dell'equazione $x^3 - 3x^2 - 18x + 40 = 0$. Sapendo che $ab = 10$, calcolare $c(a + b)$.

3.1 Successioni

Una successione è una sequenza ordinata di numeri appartenenti ad un insieme assegnato: ad esempio, si possono avere successioni di numeri interi, razionali, reali, complessi. Il primo elemento della sequenza viene, convenzionalmente, chiamato a_0 , il secondo a_1 e così via discorrendo.

I modi in cui vengono di norma descritte le successioni sono due:

1. con una legge: ciascun termine a_n è assegnato mediante una funzione che, in generale, dipende da n . Ad esempio, $a_n = 2n + 1$, $n \in \mathbb{N}$ è la successione dei numeri dispari;
2. ricorsivamente: ciascun termine a_n è assegnato mediante una funzione ricorsiva che, in generale, dipende dai termini precedenti $a_{n-1}, a_{n-2}, \dots, a_1, a_0$. Ad esempio, la successione definita da
$$\begin{cases} a_0 = a_1 = 1 \\ a_n = a_{n-1} + a_{n-2} \end{cases} \quad n > 1$$
 è la celeberrima successione di Fibonacci
1, 1, 2, 3, 5, 8, 13, ...

Una categoria che merita un più accurato esame è quella delle progressioni, successioni dipendenti linearmente dal solo termine precedente.

3.1.1 Progressioni aritmetiche

Una successione di numeri a_1, a_2, \dots, a_n si dice progressione aritmetica se è definita ricorsivamente nel seguente modo:

$$\begin{cases} a_1 = a_1 \\ a_n = a_{n-1} + d \end{cases}$$

Cioè se la differenza tra due termini consecutivi è costante ed uguale alla ragione d della progressione. Sulle progressioni aritmetiche si possono dimostrare facilmente le seguenti formule:

Il generico termine a_r si può esprimere come $a_r = a_s + (r - s)d$.

Infatti: $a_r = a_{r-1} + d = a_{r-2} + 2d = \dots = a_s + (r - s)d$.

La somma dei termini da a_r a a_s è: $S = \frac{1}{2}(a_r + a_s)(r - s + 1)$.

Infatti $a_r + a_s = (a_{r+1} - d) + (a_{s-1} + d) = a_{r+1} + a_{s-1}$, e dunque:

$$\begin{aligned} 2S &= 2(a_r + a_{r+1} + a_{r+2} + \dots + a_{s-2} + a_{s-1} + a_s) \\ &= (a_r + a_s) + (a_{r+1} + a_{s-1}) + \dots + (a_{s-1} + a_{r+1}) + (a_s + a_r) = (a_r + a_s)(r - s + 1)/2 \end{aligned}$$

Data la successione:

$$\begin{cases} a_1 = 5 \\ a_n = a_{n-1} + 7 \end{cases}$$

Scrivere il decimo termine della successione a_{10} in termini del terzo termine a_3 e calcolare la somma dei termini compresi tra questi 2.

Si ha $a_{10} = a_3 + (10 - 3) \cdot 7 = a_3 + 49$; la somma dei termini dal quarto al nono è $S = \frac{1}{2}(a_4 + a_9)(9 - 4 + 1) = \frac{1}{2}(a_1 + 21 + a_1 + 56) \cdot 6 = 246$.

3.1.2 Progressioni geometriche

Una successione di numeri a_1, a_2, \dots, a_n si dice progressione geometrica se è definita ricorsivamente nel seguente modo:

$$\begin{cases} a_1 = a_1 \\ a_n = k a_{n-1} \end{cases}$$

Cioè se il rapporto tra due termini consecutivi è costante ed uguale alla ragione k della progressione. Sulle progressioni geometriche si possono dimostrare facilmente le seguenti formule:

Il generico termine a_r si può esprimere come $a_r = a_s k^{(r-s)}$.

Infatti: $a_r = k a_{r-1} = k^2 a_{r-2} = \dots = k^{(r-s)} a_s$.

La somma dei termini da a_r a a_s è: $S = a_r \frac{k^{(s-r+1)} - 1}{k - 1}$.

Infatti: $S = a_r + a_{r+1} + a_{r+2} \dots + a_{s-1} + a_s = a_r(1 + k + k^2 + \dots + k^{(s-r-1)} + k^{(s-r)}) = a_r \frac{k^{(s-r+1)} - 1}{k - 1}$.

Il prodotto dei termini da a_r a a_s è: $P = \sqrt{(a_r \cdot a_s)^{(r-s+1)}}$.

Infatti: $a_r a_s = a_{r+1} a_{s-1}$ e, dunque, $P^2 = (a_r a_s \cdot a_{r+1} a_{s-1} \dots \cdot a_{s-1} a_{r+1} \cdot a_s a_r) = (a_r \cdot a_s)^{(r-s+1)}$.

Data la successione:

$$\begin{cases} a_1 = 5 \\ a_n = 7a_{n-1} \end{cases}$$

Scrivere il decimo termine della successione a_{10} in termini del terzo termine a_3 e calcolare la somma dei termini compresi tra questi 2. Calcolare inoltre il prodotto dei primi 3 termini.

Si ha $a_{10} = a_3 \cdot 7^{(10-3)} = a_3 \cdot 7^7$; la somma dei termini dal quarto al nono è $S = a_4 \frac{7^{(9-4+1)} - 1}{7 - 1} = 1715 \cdot \frac{117648}{6} = 33627720$.

Il prodotto dei primi 3 termini è $P = \sqrt{(a_1 \cdot a_3)^{(3-1+1)}} = \sqrt{(5 \cdot 245)^3} = 42875$.

3.1.3 Progressioni miste

Una successione di numeri a_1, a_2, \dots, a_n si dice progressione mista se non è nè geometrica, nè aritmetica, ma è definita ricorsivamente nel seguente modo:

$$\begin{cases} a_1 = a_1 \\ a_n = ka_{n-1} + d \end{cases} \quad k \neq 1, d \neq 0$$

Per le progressioni miste è valida la seguente formula, della quale omettiamo la dimostrazione:

Il generico termine a_r si può esprimere come $k^r a_0 + \frac{k^r - 1}{k - 1} d$.

Data la successione:

$$\begin{cases} a_1 = 5 \\ a_n = 7a_{n-1} + 6 \end{cases}$$

Scrivere il decimo termine della successione a_{10} in termini del terzo termine a_3 .

Si ha $a_{10} = a_3 \cdot 7^{(10-3)} + 6 \cdot \frac{7^{(10-3)} - 1}{7 - 1}$.

3.2 Polinomi

Un *polinomio* a coefficienti reali nella indeterminata X è un'espressione formale del tipo

$$a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

Al polinomio è associata in modo naturale una funzione polinomiale, più precisamente la funzione $P(x)$, che alla variabile reale x associa il numero reale

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Si definisce *grado* di un polinomio il massimo esponente della x che compare nel polinomio (cioè il massimo esponente della x il cui coefficiente correlato non è nullo). Nel caso del polinomio $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, il suo grado è n a patto che $a_n \neq 0$.

Si definisce *radice* di un polinomio un numero α tale che $P(\alpha) = 0$. Si definisce polinomio *monico* un polinomio del tipo $X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$, ovvero un polinomio di grado n che ha 1 come coefficiente di X^n .

3.2.1 Operazioni tra polinomi

Nell'insieme dei polinomi, esistono operazioni binarie il cui risultato è ancora un polinomio.

- **Somma:** per sommare due polinomi è sufficiente sommare tra loro nel modo consueto i coefficienti corrispondenti ad uguali esponenti della variabile x . Ad esempio, siano $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ e $Q(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$ due polinomi. Supponendo $n \geq m$, $P(x) + Q(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_{m+1} x^{m+1} + (a_m + b_m) x^m + (a_{m-1} + b_{m-1}) x^{m-1} + \dots + (a_1 + b_1) x + a_0 + b_0$. Appare chiaro come il grado del polinomio somma sia non più grande del grado massimo tra i due polinomi. Se i due gradi sono diversi, allora il polinomio somma ha come grado il maggiore tra i due.
- **Differenza:** analoghe considerazioni valgono per la differenza tra polinomi e per la relazione tra i gradi dei polinomi.
- **Moltiplicazione:** è possibile moltiplicare tra loro due polinomi utilizzando più volte la proprietà distributiva del prodotto rispetto alla somma. In questo caso, ciascun termine di un polinomio va moltiplicato per ciascun termine dell'altro. Il grado del polinomio prodotto è sempre uguale alla somma dei gradi dei due polinomi, come può facilmente essere provato: se il primo ha grado n e il secondo ha grado m , esiste sicuramente un termine in x^{n+m} con coefficiente non nullo.

In generale, la divisione e le altre operazioni non restituiscono come risultato un polinomio.

Dati i due polinomi $b(x) = x^6 - 2x^5 + x^4 - 9x^3 + 18x^2 - 9x + 1$ e $a(x) = x^5 - x^3 - 9x^2 + 9$, trovarne somma e prodotto.

La somma è $b(x) + a(x) = x^6 + (-2 + 1)x^5 + x^4 + (-9 - 1)x^3 + (18 - 9)x^2 - 9x + (1 + 9) = x^6 - x^5 + x^4 - 10x^3 + 9x^2 - 9x + 10$; il prodotto è $b(x) \cdot a(x) = x^6(x^5 - x^3 - 9x^2 + 9) - 2x^5(x^5 - x^3 - 9x^2 + 9) + x^4(x^5 - x^3 - 9x^2 + 9) - 9x^3(x^5 - x^3 - 9x^2 + 9) + 18x^2(x^5 - x^3 - 9x^2 + 9) - 9x(x^5 - x^3 - 9x^2 + 9) + (x^5 - x^3 - 9x^2 + 9) = x^{11}(1) + x^{10}(-2) + x^9(-1 + 1) + x^8(-9 + 2 - 9) + x^7(18 - 1 + 18) + x^6(9 - 9 + 9 - 9) + x^5(-18 + 81 - 18 + 1) + x^4(9 - 162 + 9) + x^3(-81 + 81 - 1) + x^2(162 - 9) + x(-81) + 9 = x^{11} - 2x^{10} - 16x^8 + 35x^7 + 46x^5 - 144x^4 - x^3 + 153x^2 - 81x + 9$.

3.2.2 Divisione euclidea tra polinomi

Come con i numeri naturali, così è possibile effettuare la divisione euclidea tra due polinomi. In particolare, se $a(x)$ e $b(x)$ sono due polinomi, allora esistono e sono unici due polinomi $q(x)$ e $r(x)$ tali che:

- $b(x) = a(x) \cdot q(x) + r(x)$;
- il grado di $r(x)$ è minore del grado di $q(x)$.

Per ottenere i due suddetti polinomi si può effettuare una normale divisione in colonna, nel corso della quale ad ogni passaggio si eguaglia il termine di grado massimo per permetterne la semplificazione. Per trovare l'MCD tra due polinomi si esegue lo stesso procedimento (algoritmo di Euclide) usato per i numeri naturali.

Dati i polinomi $b(x) = x^6 - 2x^5 + x^4 - 9x^3 + 18x^2 - 9x + 1$ e $a(x) = x^5 - x^3 - 9x^2 + 9$, eseguire la divisione per determinare $q(x)$ e $r(x)$ tali che $b(x) = a(x) \cdot q(x) + r(x)$ e calcolare, mediante l'algoritmo di Euclide, il massimo comun divisore tra $a(x)$ e $b(x)$.

$$\begin{array}{r|rrrrrr}
 x^6 & -2x^5 & x^4 & -9x^3 & 18x^2 & -9x & 1 & x^5 & -x^3 & -9x^2 & 9 \\
 x^6 & & -x^4 & -9x^3 & & 9x & & x & -2 & & \\
 \hline
 & -2x^5 & 2x^4 & & 18x^2 & -18x & 1 & & & & \\
 & -2x^5 & & 2x^3 & 18x^2 & & -18 & & & & \\
 \hline
 & & 2x^4 & -2x^3 & & -18x & 19 & & & &
 \end{array}$$

Per determinare l'MCD tra i polinomi dati, occorre procedere con divisioni successive:

$$(x^6 - 2x^5 + x^4 - 9x^3 + 18x^2 - 9x + 1) = (x^5 - x^3 - 9x^2 + 9)(x - 2) + (2x^4 - 2x^3 - 18x + 19)$$

$$(x^5 - x^3 - 9x^2 + 9) = (2x^4 - 2x^3 - 18x + 19)\left(\frac{1}{2}x + \frac{1}{2}\right) + \left(-\frac{1}{2}x - \frac{1}{2}\right)$$

$$(2x^4 - 2x^3 - 18x + 19) = \left(-\frac{1}{2}x - \frac{1}{2}\right)(-4x^3 + 8x^2 - 8x + 44) + 41$$

L'algoritmo di Euclide restituisce 41 come risposta: questo significa che i due polinomi non hanno in comune nessun polinomio di primo grado o di grado superiore al primo, dunque che sono primi tra loro.

3.2.3 Scomponibilità di polinomi

Un nodo cruciale nella teoria dei polinomi è certamente la loro scomposizione. Se eseguire una moltiplicazione tra polinomi è piuttosto semplice, non altrettanto si può dire dell'operazione inversa, analogamente con quanto accade per la scomposizione in fattori primi dei numeri interi.

La scomposizione varia a seconda dell'insieme di appartenenza dei coefficienti. In particolare, un polinomio che non può essere espresso come prodotto di due polinomi aventi grado maggiore di 1 si dice *irriducibile*, altrimenti è detto *riducibile*. Valgono i seguenti risultati:

- Se l'insieme considerato è quello dei numeri razionali \mathbb{Q} , è possibile scomporlo tramite le radici razionali, le quali possono essere trovate in maniera piuttosto agevole (cfr. 3.2.5). Inoltre, si può provare che, dato $f(x) = a_n x^n + \dots + a_0$ polinomio a coefficienti interi, se esiste un primo p tale che p non divide a_n , p divide i coefficienti a_{n-1}, \dots, a_0 e p^2 non divide a_0 , allora $f(x)$ è irriducibile in $\mathbb{Q}[x]$: questo risultato è noto come criterio di Eisenstein. Purtroppo non esiste una caratterizzazione dei polinomi irriducibili: ne esistono di qualsiasi grado (ad esempio, $p(x) = x^n + 2$ è irriducibile per qualsiasi scelta di n).
- Se l'insieme considerato è quello dei numeri reali \mathbb{R} , ogni polinomio è sempre riducibile come prodotto di più polinomi irriducibili di grado 1 oppure di grado 2 con discriminante negativo. Purtroppo non esiste un procedimento che, a priori, permetta tale scomposizione.
- Se l'insieme considerato è quello dei numeri complessi \mathbb{C} , ogni polinomio è sempre riducibile come prodotto di più polinomi irriducibili di primo grado. Questo fatto è noto come *teorema fondamentale dell'algebra*.

Inoltre è opportuno conoscere queste regole pratiche:

1. Un polinomio di primo grado è sempre irriducibile.
2. Per i polinomi di secondo grado esiste una formula che consente di calcolare le relative radici (e quindi scomporre il polinomio): se $P(x) = ax^2 + bx + c$, le radici sono $\frac{-b + \sqrt{b^2 - 4ac}}{2a}$ e $\frac{-b - \sqrt{b^2 - 4ac}}{2a}$. La quantità $b^2 - 4ac$ è detta *discriminante* e, nel caso in cui questo sia negativo, il polinomio non ammette soluzioni reali.
3. Ogni polinomio con coefficienti razionali può essere ricondotto ad un polinomio con coefficienti interi: basta moltiplicare per il minimo comune multiplo dei denominatori.

Prodotti notevoli

In generale, scomporre un polinomio non è un compito agevole, ma si rende spesso necessario per la risoluzione dei problemi. È bene perciò tenere presenti i cosiddetti prodotti notevoli, cioè espressioni polinomiali che possono essere facilmente scomposte.

- $(x^2 - a^2) = (x + a)(x - a)$;
- $(x^3 \pm a^3) = (x \pm a)(x^2 + a^2 \mp ax)$;
- $(x \pm a)^2 = x^2 + a^2 \pm 2ax$;
- $(x \pm a)^3 = x^3 \pm 3ax^2 + 3a^2x \pm a^3$;
- $(ax^2 + bx + c) = (x - \frac{-b + \sqrt{b^2 - 4ac}}{2a})(x - \frac{-b - \sqrt{b^2 - 4ac}}{2a})$.

Generalizzando:

- $(x^{2n} - a^{2m}) = (x^n + a^m)(x^n - a^m)$;
- $(x^{2n+1} \mp a^{2n+1}) = (x \mp a)(x^{2n} \pm x^{2n-1}a + x^{2n-2}a^2 \pm x^{2n-3}a^3 + \dots + x^2a^{2n-2} \pm xa^{2n-1} + a^{2n})$;
- $(a + x)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}x + \binom{n}{2}a^{n-2}x^2 + \dots + \binom{n}{n-1}ax^{n-1} + \binom{n}{n}x^n = \sum_{k=0}^n \binom{n}{k}a^{n-k}x^k$ (cfr 4.1).

3.2.4 Principio di identità dei polinomi

Due polinomi

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

e

$$Q(X) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$$

si dicono uguali se le loro funzioni polinomiali coincidono, ovvero

$$n = m, a_n = b_m, \dots, a_1 = b_1, a_0 = b_0$$

Questo è noto come *principio di identità dei polinomi*.

Esiste inoltre un criterio per asserire che $P(X)$ coincide con $Q(X)$: è sufficiente verificare che i valori assunti da $P(x)$ e $Q(x)$ siano gli stessi per almeno $n + 1$ valori distinti di x (supponendo $n \geq m$).

Il principio di identità dei polinomi, come pure il criterio appena enunciato, è valido anche in campo complesso ed è valido anche se le indeterminate sono due o più.

Siano $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ e $Q(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$ due polinomi di grado n . Inoltre, $P(2k\pi) = Q(2k\pi)$ per $0 \leq k \leq n$. I due polinomi coincidono?

I due polinomi hanno $n + 1$ valori distinti nei quali assumono lo stesso valore: questo è sufficiente ad asserire che i due polinomi sono in realtà coincidenti.

3.2.5 Radici razionali dei polinomi

Se $P(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$ è un polinomio a coefficienti interi e $x = p/q$ è una sua radice razionale, cioè una soluzione dell'equazione $P(x) = 0$ con p, q interi e primi tra loro (frazione ridotta ai minimi termini), allora:

1. q divide a_0 ;
2. p divide a_n .

Questa limitazione permette di stabilire (a tentativi) quante soluzioni razionali ha un'equazione a coefficienti interi (o eventualmente razionali).

Dato il polinomio $p(x) = x^4 - 4x^3 + 7x^2 - 16x + 12$, determinarne tutte le radici razionali.

Se esiste una radice razionale, allora essa appartiene all'insieme dei divisori di 12, cioè $\{1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12\}$.

A tentativi si prova che $p(1) = p(3) = 0$ e dunque, eseguendo la divisione tra polinomi, si arriva a $p(x) = (x - 3)(x - 1)(x^2 + 4)$. poiché nessun altro elemento dell'insieme è radice del polinomio, le uniche radici razionali sono le due trovate. D'altronde, una volta giunti

a $x^2 + 4$, sarebbe stato possibile determinare direttamente le radici rimanenti con la nota formula e verificare la loro irrazionalità.

3.2.6 Teorema di Ruffini

Un polinomio $P(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ è divisibile per un binomio $(x - \alpha)$ se e solo se α è radice di $P(x)$.

Se $P(x)$ ha radici $\alpha_1, \alpha_2, \dots, \alpha_s$ rispettivamente di molteplicità k_1, k_2, \dots, k_s , con $k_1 + k_2 + \dots + k_s = n$, allora $P(x)$ si può scomporre in fattori lineari come:

$$P(x) = a_0(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \dots (x - \alpha_s)^{k_s}.$$

Dato il polinomio $p(x) = x^4 - 4x^3 - x^2 + 16x - 12$, scomporlo in fattori lineari.

Le radici vanno cercate nell'insieme $\{1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12\}$; a tentativi, si verifica che $p(1) = p(2) = p(-2) = p(3) = 0$, e dunque il polinomio dato può essere scomposto, come si può verificare mediante divisioni successive, in $p(x) = (x - 1)(x - 2)(x + 2)(x - 3)$.

3.2.7 Relazioni tra radici e coefficienti dei polinomi

Sia $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ un polinomio monico di grado n . Siano $\lambda_1, \lambda_2, \dots, \lambda_n$ le sue radici (in generale complesse), ripetute secondo la loro molteplicità; allora

$$\begin{aligned} -a_{n-1} &= \sum_{1 \leq i \leq n} \lambda_i \\ a_{n-2} &= \sum_{1 \leq i < j \leq n} \lambda_i \cdot \lambda_j \\ -a_{n-3} &= \sum_{1 \leq i < j < k \leq n} \lambda_i \cdot \lambda_j \cdot \lambda_k \\ &\vdots \\ (-1)^n a_0 &= \lambda_1 \cdot \lambda_2 \cdot \dots \cdot \lambda_n \end{aligned}$$

Nel caso in cui il polinomio non sia monico, basta dividere il polinomio per il coefficiente di grado massimo e ricondursi al caso precedente. Anche le somme di potenze di radici hanno delle regolarità particolari, infatti se poniamo $S_k = \lambda_1^k + \lambda_2^k + \dots + \lambda_n^k$ avremo che

$$\begin{aligned} 1 \leq k \leq n: & \quad S_k + a_{n-1}S_{k-1} + \dots + a_{n-k}k = 0; \\ n \leq k: & \quad S_k + a_{n-1}S_{k-1} + \dots + a_0S_{k-n} = 0. \end{aligned}$$

Nel caso di $n = 2, 3$ abbiamo inoltre alcune formule per calcolare le somme di potenze di radici:

$$\begin{aligned} n=2: & \quad S_1 = -a_1, \quad S_2 = a_1^2 - 2a_0; \\ n=3: & \quad S_1 = -a_2, \quad S_2 = a_2^2 - 2a_1, \quad S_3 = -a_2^3 + 3a_1a_2 - 3a_0. \end{aligned}$$

Dato il polinomio $p(x) = 7x^3 + 2x + 1$, calcolare S_1 , S_2 e S_3 .

Occorre trasformare il polinomio dato in uno monico. Sia dunque $\tilde{p}(x) = x^3 + \frac{2}{7}x + \frac{1}{7}$.

Utilizzando le formule si ottiene

$$S_1 = -a_2 = 0,$$

$$S_2 = a_2^2 - 2a_1 = -2\left(\frac{2}{7}\right) = \frac{-4}{7},$$

$$S_3 = -a_2^3 + 3a_1a_2 - 3a_0 = -3\left(\frac{1}{7}\right) = \frac{-3}{7}.$$

Soluzione problema di inizio capitolo.

Utilizzando le relazioni tra radici e coefficienti dei polinomi, non è necessario conoscere esplicitamente le radici.

Il polinomio in questione, $x^3 - 3x^2 - 18x + 40 = 0$, è monico e le radici sono a, b, c . Si ottiene $-3 = -(a + b + c)$, $-18 = ab + ac + bc$ e $40 = -abc$. Sostituendo il dato $ab = 10$ nella seconda delle tre equazioni si ricava $-18 = ab + ac + bc = 10 + c(a + b)$ e quindi $c(a + b) = -28$.

3.3 Disuguaglianze

3.3.1 Disuguaglianze tra le medie

Dato un insieme $A = a_1, a_2, \dots, a_n$ di n numeri qualsiasi (solitamente $\subset \mathbb{R}$), rientra in qualsiasi corso di studio l'apprendimento della nozione di *media aritmetica*, definita come $AM = \frac{a_1 + a_2 + \dots + a_n}{n} = \frac{\sum_{i=1}^n a_i}{n}$. Essa ha la naturale proprietà di essere una "via di mezzo" tra tutti gli elementi dell'insieme A .

Esistono però infinite diverse medie ed è possibile dimostrare una relazione che intercorre tra tutte queste. In particolare, le medie più importanti (ed usate) sono:

- La *media geometrica*: $GM = \sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n} = \sqrt[n]{\prod_{i=1}^n a_i}$
- La *media armonica*: $HM = \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n}}$

Inoltre, definiamo con un leggero abuso di scrittura altre due medie:

- $M_{-\infty} = \min_{i=1, \dots, n} a_i$
- $M_{+\infty} = \max_{i=1, \dots, n} a_i$

Vale la seguente relazione:

$$M_{-\infty} \leq HM \leq GM \leq AM \leq M_{+\infty}$$

Inoltre sussiste la relazione di eguaglianza se e solo se tutti gli a_i sono uguali.

Dato l'insieme $A = 2, 4, 7, 9, 12$, determinarne la media geometrica, la media aritmetica e la media armonica e verificare che sia soddisfatta la disuguaglianza tra le medie.

Utilizzando le formule:

- $AM = \frac{2+4+7+9+12}{5} = 6,8$;
- $GM = \sqrt[5]{2 \cdot 4 \cdot 7 \cdot 9 \cdot 12} \approx 5,71$;
- $HM = \frac{5}{\frac{1}{2} + \frac{1}{4} + \frac{1}{7} + \frac{1}{9} + \frac{1}{12}} \approx 4,60$.

In effetti, $4,60 \leq 5,71 \leq 6,8$.

3.3.2 Disuguaglianza di riarrangiamento

Siano a_1, a_2, \dots, a_n e b_1, b_2, \dots, b_n due insiemi di numeri reali e supponiamo, senza perdere di generalità, che gli elementi siano ordinati in modo che $a_1 \leq a_2 \leq \dots \leq a_n$ e $b_1 \leq b_2 \leq \dots \leq b_n$. Supponiamo ora di associare, ad ogni a_i , un b_j in modo da creare una corrispondenza biunivoca tra i due insiemi: in questo modo creiamo n coppie (a_i, b_j) in modo che un elemento qualunque dei due insiemi compaia una e una sola volta in una coppia. Considerando la sommatoria $\sum_{\text{coppie}} (a_i \cdot b_j)$, valgono le seguenti due proprietà:

- $\sum_{\text{coppie}} (a_i \cdot b_j)$ è massima quando ad a_1 è associato l'elemento b_1 , ad a_2 è associato b_2 e via discorrendo;
- $\sum_{\text{coppie}} (a_i \cdot b_j)$ è minima quando ad a_1 è associato l'elemento b_n , ad a_2 è associato b_{n-1} e via discorrendo.

Sostanzialmente, per avere somma massima occorre associare il più piccolo con il più piccolo, il secondo più piccolo con il più piccolo e così via; per avere somma minima occorre, viceversa, associare il più piccolo con il più grande, il secondo più piccolo con il secondo più grande e così via.

Dati i due insiemi $A = \{x/x \in \mathbb{N}, x \text{ è pari}, x < 10\}$ e $B = \{x/x \in \mathbb{N}, x \text{ è dispari}, x < 10\}$, determinare il massimo e il minimo della somma $\sum_{\text{coppie}} (a_i \cdot b_j)$ con $a_i \in A, b_j \in B$.

Utilizzando la disuguaglianza di riarrangiamento, si ha che il massimo è $9 \cdot 8 + 7 \cdot 6 + 5 \cdot 4 + 3 \cdot 2 + 1 \cdot 0 = 140$ e che il minimo è $9 \cdot 0 + 7 \cdot 2 + 5 \cdot 4 + 3 \cdot 6 + 1 \cdot 8 = 60$.

3.3.3 Disuguaglianza triangolare

Siano a e b due numeri reali. Allora vale la seguente disuguaglianza (disuguaglianza triangolare):

$$\left| |a| - |b| \right| \leq |a \pm b| \leq |a| + |b|$$

Inoltre, se a e b sono intese come quantità vettoriali, le precedenti relazioni continuano a valere (purché al valore assoluto si sostituisca la norma di un vettore) ed acquistano un significato geometrico (cfr 5.4.1).

3.4 Approfondimenti

3.4.1 Basi di numerazione

Adottando la notazione posizionale nella scrittura degli interi, la base di numerazione b è un numero naturale positivo che rappresenta la quantità di simboli diversi che si hanno a disposizione per scrivere un intero. La base con la quale si è soliti ragionare è la base 10: ogni numero è ottenuto come sequenza di cifre scelte tra le 10 a disposizione, eventualmente ripetute. In particolare ogni numero intero si può scrivere come un polinomio in b in cui le cifre sono i coefficienti. In particolare chiamando C_1, \dots, C_n le cifre di un numero in base b il numero sarà: $C_1 \cdot b^{(n-1)} + C_2 \cdot b^{(n-2)} + \dots + C_n \cdot b^0$. Per esempio il numero 123 si può scrivere in base 10 come $1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$, in base 2 invece si può scrivere come $1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$ cioè 111101, mentre in base 16 (dove le cifre sono 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F) si scrive come $7 \cdot 16 + 11$ cioè 7B.

3.4.2 Dalla base b alla base 10

Per trasformare un numero scritto in base b in uno scritto in base 10 è sufficiente scrivere il polinomio in b e calcolarne il risultato.

Scrivere il numero $(11010101)_2$ in base 10.

$$(11010101)_2 = 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 2^7 + 2^6 + 2^4 + 2^2 + 1 = 213.$$

3.4.3 Dalla base 10 alla base b

Per trasformare un numero scritto in base 10 in uno scritto in base b è sufficiente fare:

$$n \text{ div } b = a_1 \quad \text{resto } r_1$$

$$a_1 \text{ div } b = a_2 \quad \text{resto } r_2$$

$$a_2 \text{ div } b = a_3 \quad \text{resto } r_3$$

...

$$a_{n-1} \text{ div } b = a_n \quad \text{resto } r_n$$

fino a che $a_n = 0$. A quel punto basta usare i resti r_1, \dots, r_n come cifre del numero dove r_1 è la cifra delle unità, r_2 delle decine e così via.

Scrivere il numero 213 in base 2.

$$213 \text{ div } 2 = 106 \quad \text{resto } 1$$

$$106 \text{ div } 2 = 53 \quad \text{resto } 0$$

$$53 \text{ div } 2 = 26 \quad \text{resto } 1$$

$$26 \text{ div } 2 = 13 \quad \text{resto } 0$$

$$13 \text{ div } 2 = 6 \quad \text{resto } 1$$

$$6 \text{ div } 2 = 3 \quad \text{resto } 0$$

$$3 \text{ div } 2 = 1 \quad \text{resto } 1$$

$$1 \text{ div } 2 = 0 \quad \text{resto } 1$$

Il numero pertanto sarà $(11010101)_2$.

3.4.4 Numeri decimali

Anche i numeri decimali razionali si possono scrivere in basi diverse mantenendo la stessa regola descritta in precedenza per passare dalla base b alla base 10, considerando le cifre dopo la virgola come se fossero esponenti negativi da dare alle potenze della base; passare dalla base 10 ad una base b è invece molto più difficoltoso.

3.4.5 Successioni per ricorrenza lineari

Nella successione

$$\begin{cases} x_0 = x_0 \\ x_1 = x_1 \\ x_{n+1} = \alpha \cdot x_n + \beta \cdot x_{n-1} \end{cases}$$

sono dati i primi due termini, e ciascuno dei successivi dipende dai due termini immediatamente precedenti. Esiste un metodo per scrivere il termine generico x_r in modo che dipenda solo da r . Si risolve innanzitutto l'equazione $x^2 - \alpha x - \beta = 0$. Se le due soluzioni S_1 e S_2 sono distinte, allora si può dimostrare che

$$x_r = a \cdot S_1^r + b \cdot S_2^r$$

con a e b coefficienti opportuni. Per trovare a e b , si sostituisce prima $r = 0$ e poi $r = 1$ nell'espressione di x_r , ottenendo un sistema di due equazioni in a, b , che si risolve utilizzando i valori noti di x_0 e x_1 . Se invece le soluzioni coincidono, cioè se $S_1 = S_2 = S$, allora si può dimostrare che

$$x_r = a \cdot S^r + b \cdot r \cdot S^r$$

con a e b coefficienti opportuni che si determinano come nel caso precedente.

Data la seguente successione, detta successione di Fibonacci:

$$\begin{cases} x_0 = 0 \\ x_1 = 1 \\ x_{n+1} = x_n + x_{n-1} \end{cases}$$

ricavare l'espressione del termine generico x_r

Si tratta della successione 0, 1, 1, 2, 3, 5, 8, 13, 21, ... Qui $\alpha = \beta = 1$, quindi si deve risolvere dapprima $x^2 - x - 1 = 0$. Le soluzioni sono diverse: $S_1 = \frac{1+\sqrt{5}}{2}$ e $S_2 = \frac{1-\sqrt{5}}{2}$. Quindi $x_r = a \cdot \left(\frac{1+\sqrt{5}}{2}\right)^r + b \cdot \left(\frac{1-\sqrt{5}}{2}\right)^r$. Se $r = 0$ allora $0 = a + b$ cioè $b = -a$; se $r = 1$ allora $1 = a \cdot \left(\frac{1+\sqrt{5}}{2}\right) + b \cdot \left(\frac{1-\sqrt{5}}{2}\right) = a \cdot \left(\frac{1+\sqrt{5}}{2}\right) - a \cdot \left(\frac{1-\sqrt{5}}{2}\right) = a\sqrt{5}$ e quindi $a = \frac{1}{\sqrt{5}}$ e $b = -\frac{1}{\sqrt{5}}$. Si può scrivere ora:

$$x_r = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^r - \left(\frac{1-\sqrt{5}}{2} \right)^r \right)$$

Nota bene: sommando numeri naturali si ottengono numeri naturali, quindi nonostante compaiano radici nell'espressione di x_r , queste si semplificano sempre quando si sviluppano le potenze.

Data la seguente successione:

$$\begin{cases} x_0 = 0 \\ x_1 = 1 \\ x_{n+1} = 5x_n - 6x_{n-1} \end{cases}$$

ricavare l'espressione del termine generico x_r .

Si tratta della successione 0, 1, 5, 19, 65, ... Qui $\alpha = 5$ e $\beta = -6$, quindi si deve risolvere dapprima $x^2 - 5x + 6 = 0$. Le soluzioni sono diverse: $S_1 = 3$ e $S_2 = 2$. Quindi $x_r = a \cdot 3^r + b \cdot 2^r$. Se $r = 0$ allora $0 = a + b$ cioè $b = -a$; se $r = 1$ allora $1 = 3a + 2b = 3a - 2a = a$ e quindi $a = 1$ e $b = -1$. Segue che $x_r = 3^r - 2^r$.

Data la seguente successione:

$$\begin{cases} x_0 = 2 \\ x_1 = 21 \\ x_{n+1} = 6x_n - 9x_{n-1} \end{cases}$$

calcolare $\frac{x_{88}}{3^{88}}$.

Conviene scrivere il termine generico. $\alpha = 6$ e $\beta = -9$; l'equazione $x^2 - 6x + 9 = (x - 3)^2 = 0$ ha due soluzioni coincidenti $S_1 = S_2 = S = 3$. Quindi $x_r = a \cdot 3^r + b \cdot r \cdot 3^r$. Se $r = 0$ allora $2 = a$; se $r = 1$ allora $21 = 3a + 3b = 6 + 3b$ e quindi $a = 2$ e $b = 5$. Segue che $x_r = 2 \cdot 3^r + 5 \cdot r \cdot 3^r = (2 + 5r) \cdot 3^r$. Per trovare il risultato basta adesso sostituire $r = 88$, ottenendo $x_{88} = 442 \cdot 3^{88}$ e $\frac{x_{88}}{3^{88}} = 442$.

3.5 Esercizi

3.5.1 Esercizi di base

Successioni

1. Data la successione: $\begin{cases} a_1 = 3 \\ a_n = 2 + a_{n-1} \end{cases}$
 - a) calcolare la somma dei primi 7 termini;
 - b) esprimere, mediante il terzo termine della successione, a_7 .

2. Data la successione: $\begin{cases} a_1 = 5 \\ a_n = a_{n-1} - 1 \end{cases}$
 - a) calcolare la somma dei primi 11 termini;
 - b) esprimere, mediante il quinto termine della successione, a_{12} .

3. Data la successione: $\begin{cases} a_1 = 3 \\ a_n = -a_{n-1} \end{cases}$
 - a) calcolare la somma dei primi 10 termini;
 - b) calcolare la somma dei termini dal k -esimo al $(k+4)$ -esimo, con k pari;
 - c) calcolare il prodotto dei primi 4 termini;
 - d) esprimere, mediante il secondo termine della successione, a_5 .

4. Data la successione: $\begin{cases} a_1 = 3 \\ a_n = \frac{a_{n-1}}{2} \end{cases}$
 - a) calcolare la somma dei primi 7 termini;
 - b) calcolare la somma dei termini dal terzo al sesto;
 - c) calcolare il prodotto dei primi 4 termini;
 - d) calcolare il prodotto dei termini dal terzo al sesto;
 - e) esprimere, mediante il secondo termine della successione, a_5 .

5. Data la successione: $\begin{cases} a_1 = 3 \\ a_n = \frac{a_{n-1}}{2} + 1 \end{cases}$
 - a) calcolare la somma dei primi 4 termini;
 - b) esprimere, mediante il secondo termine della successione, a_{10} .

Polinomi

6. Dati i due polinomi $p(x) = x^5 + 3x^4 + x^3 - 4x^2 + 7x + 6$ e $q(x) = x^4 - x^2 - x + 4$, trovarne la somma, la differenza e il prodotto.
7. Dati i due polinomi $p(x) = x^5 + 3x^4 + x^3 - 4x^2 + 7x + 6$ e $q(x) = x^4 - x^2 - x + 4$, trovarne il massimo comune divisore con l'algoritmo di Euclide, mediante divisioni successive.

8. Dati i due polinomi $p(x) = x^7 + 3x^6 - x^5 + 3x^3 - 2x^2 - 4x$ e $q(x) = x^3 - x$, trovarne il massimo comune divisore con l'algoritmo di Euclide, mediante divisioni successive.
9. Dato il polinomio $p(x) = x^7 + 3x^6 - x^5 + 3x^3 - 2x^2 - 4x$, trovarne tutte le radici razionali.
10. Dato il polinomio $p(x) = x^5 + 3x^4 + x^3 - 4x^2 + 7x + 6$, trovarne tutte le radici razionali.
11. Scomporre in fattori lineari, se possibile, il polinomio $p(x) = x^4 + 2x^3 - 22x^2 - 14x + 105$.
12. Scomporre in fattori lineari, se possibile, il polinomio $p(x) = x^4 - 7x^2 - 8$.
13. Scomporre in fattori lineari, se possibile, il polinomio $p(x) = x^5 + 13x^4 + 10x^3 - 14x^2 - 3x + 9$.
14. Dato il polinomio $p(x) = x^4 + 3x^3 - x^2 - 9x + 6$, dette $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ le sue radici, calcolare il valore dell'espressione $\frac{1}{\lambda_1\lambda_2\lambda_3} + \frac{1}{\lambda_1\lambda_2\lambda_4} + \frac{1}{\lambda_1\lambda_3\lambda_4} + \frac{1}{\lambda_2\lambda_3\lambda_4}$.
15. Dato il polinomio $p(x) = \sqrt{3}x^3 + \pi x^2 - \frac{2}{3}x - 2$, dette $\lambda_1, \lambda_2, \lambda_3$ le sue radici, calcolare il valore dell'espressione $\lambda_1^2(\lambda_1 - 1) + \lambda_2^2(\lambda_2 - 1) + \lambda_3^2(\lambda_3 - 1)$.

Disuguaglianze

16. Dati i due insiemi $A = \{4, 11, 12, -2\}$ e $B = \{-4, 2, 5, 7\}$, trovare massimo e minimo della somma $\sum_{\text{coppie}}(a_i \cdot b_j)$ con $a_i \in A, b_j \in B$. Trovare inoltre la media aritmetica, geometrica ed armonica dell'insieme dato.
17. Dati i due insiemi $A = \{-2, -4, -6\}$ e $B = \{-1, 2, 3\}$, trovare massimo e minimo della somma $\sum_{\text{coppie}}(a_i \cdot b_j)$ con $a_i \in A, b_j \in B$. Trovare inoltre la media aritmetica, geometrica ed armonica dell'insieme dato.

3.5.2 Esercizi svolti

1. Trova la somma algebrica dei coefficienti del polinomio:
 $(x^{21} + 4x^2 - 3)^{2001} - (x^{21} + 4x^2 + 3)^{667} + x^{21} + 4x^2$.
2. Sia $P(x)$ un polinomio che ha come coefficienti 0 o +1. Quale delle seguenti alternative è certamente falsa?
(A) $P(2) = 51$ **(B)** $P(3) = 92$ **(C)** $P(5) = 150$ **(D)** $P(3) = 37$
(E) $P(4) = 20$
3. Se m, n e 1 sono le tre radici dell'equazione $x^3 - mx^2 + nx - 1 = 0$, allora quanto vale la loro somma?
(A) -1 **(B)** 0 **(C)** 1 **(D)** 3 **(E)** 2
4. Quante radici reali possiede l'equazione $9 - 2^x = 2^{3-x}$?
(A) due **(B)** più di due ma un numero finito **(C)** nessuna
(D) infinite **(E)** una

5. Ad una festa l'età media è di 31 anni, l'età media degli uomini è 35 anni e l'età media delle donne è 25 anni. Qual è il rapporto tra il numero degli uomini e quello delle donne?
 (A) $\frac{5}{7}$ (B) $\frac{7}{5}$ (C) $\frac{4}{3}$ (D) $\frac{3}{2}$ (E) 2
6. Per quali valori di λ , l'equazione $||x| - 1| = \lambda$ ha esattamente 3 soluzioni?
 (A) $\lambda = 0$ (B) $\lambda = 1$ (C) $\lambda \geq 1$ (D) $0 \leq \lambda \leq 1$ (E) $\lambda \geq 0$
7. Per quanti valori del parametro reale k il sistema

$$\begin{cases} 2x + y = 1 \\ 8x^3 + y^3 = k \end{cases}$$
 ha una e una sola soluzione reale?
 (A) 1 (B) 2 (C) 3 (D) 6 (E) non si può determinare
8. Quanti sono i numeri naturali che in base 10 si scrivono con 3 cifre e in base 2 si scrivono con 7 cifre?
9. Sia $P(X) = aX^2 + bX + c$ un polinomio di secondo grado con coefficienti reali (cioè a, b, c sono numeri reali e $a \neq 0$). Se $P(2000) = 2000$ e $P(2001) = 2001$, allora $P(2002)$ non può essere uguale a:
 (A) 2000 (B) 2001 (C) 2002 (D) 2003 (E) 2004
10. Qual è il minimo valore dell'espressione $x^2 - 8xy + 19y^2 - 6y + 14$ al variare di x e y fra i numeri reali?

3.5.3 Esercizi proposti

1. Sia a_n la successione così definita: $\begin{cases} a_0 = x \\ a_n = 2a_{n-1} - 1 \end{cases}$. Sapendo che $a_{2000} = 2^{2001} + 1$, quanto vale x ?
2. Determinare quante sono le soluzioni intere positive dell'equazione $x^x - 2^x - x^2 = 10$.
3. Determinare quante sono le coppie di interi positivi (x, y) che verificano l'equazione

$$x^2 + y^2 - 2004x - 2004y + 2xy - 2005 = 0$$

4. Trovare tutte le coppie (p, q) di numeri primi (positivi) tali che l'equazione

$$x^2 - (6p - 4q)x + 3pq = 0$$

abbia due radici intere.

5. Determinare quanto vale $\sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}}$.
6. La rappresentazione in base 2 di un numero a è 1110000100111010101110100001. Qual è la settima cifra da sinistra delle rappresentazione di a in base 8?

7. Sia $p(x) = x^{20} + a_{19}x_{19} + a_{18}x_{18} + \dots + a_1x + a_0$ un polinomio, con gli a_i interi. Sappiamo che, per tutti gli interi k compresi tra 1 e 20, $p(k) = 2k$. Quali sono le ultime tre cifre di $p(21)$?
8. Indicando con x_1, x_2, x_3, x_4 le soluzioni dell'equazione $x^4 - 2x^3 - 7x^2 - 2x + 1 = 0$, quanto vale la somma dei reciproci delle soluzioni?
9. Sia x la più piccola delle due soluzioni dell'equazione $x^2 - 4x + 2 = 0$. Determinare le prime tre cifre dopo la virgola nella scrittura (in base 10) del numero

$$x + x^2 + x^3 + \dots + x^{2009}$$

10. Sia $P(x)$ un polinomio a coefficienti interi. Se $P(3) = 5$ e $P(n^3) = 15$ per un certo numero naturale n , quanti sono i possibili valori di n ?
11. Dalle passate olimpiadi[3]: ALG75, ALG77, ALG83, ALG85, ALG86, ALG87, ALG89, ALG96.

CAPITOLO 4

Combinatoria

La *combinatoria*, nella classificazione dei problemi olimpici, si occupa dello studio dei conteggi (e quindi delle cardinalità degli insiemi) e delle probabilità: proprio per calcolare queste ultime è infatti spesso richiesto un non facile uso del calcolo combinatorio.

Uno dei concorsi più in voga tra gli italiani, anche grazie allo spazio dedicato ad esso dalla televisione e dai giornali, è il SuperEnalotto. Esso consiste nell'estrazione di 6 numeri, da 1 a 90, più due numeri supplementari, che permettono di ottenere alcuni tipi di vincite. Il premio più importante è però quello che si ottiene indovinando tutti e sei i numeri principali. Non di rado si sente parlare della difficoltà di ottenere questa vincita, fatto confermato dal ricco montepremi che si accumula estrazione dopo estrazione, per il calcolo della relativa probabilità vengono chiamati in causa presunti recenti studi e calcoli complicatissimi, ma, più concretamente, come si fa a calcolare questa possibilità?

Subito un'osservazione: non è necessario alcun calcolo complicatissimo, nè sono stati svolti recenti studi, per ottenere tale risultato. Al contrario, si tratta di un risultato elementare del calcolo combinatorio. Questo è un esempio di problema che ne richiede l'uso, in quanto consiste nel contare un numero di oggetti definiti in un certo modo. Viene richiesto il calcolo di una probabilità; non tutti i problemi di combinatoria ne richiedono uno, ma molti sono legati a questo argomento. Quello che segue è ciò che può servire per le gare nell'ambito delle Olimpiadi di Matematica.

4.1 Premesse per il calcolo combinatorio

In matematica, se n è un intero positivo, si definisce n fattoriale e si indica con $n!$ il prodotto di n numeri interi decrescenti a partire da n .

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 1$$

Risulta ovvio a partire dalla definizione che vale la relazione:

$$n! = n \cdot (n-1)!$$

cioè che per calcolare il fattoriale di un numero n basta moltiplicare per n il fattoriale del numero precedente. In questo modo è possibile calcolare qualsiasi fattoriale se si aggiunge l'informazione di base che $0! = 1$. Si definisce invece come *coefficiente binomiale* l'espressione:

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

Per esempio $\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5!}{3!2!} = 10$.

Per i coefficienti binomiali valgono alcune interessanti proprietà:

$$\binom{n}{k} = \frac{n}{k} \cdot \binom{n-1}{k-1}$$

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

$$\binom{n}{k} = \binom{n}{n-k}$$

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

Tramite l'uso dei coefficienti binomiali è stato ottenuto un risultato molto importante che è il *binomio di Newton*, cioè la formula che esprime lo sviluppo della potenza n -esima di un binomio:

$$(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n$$

Che in forma più concisa diventa:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

I coefficienti binomiali hanno quindi il ruolo dei coefficienti del polinomio, ed è infatti questa la ragione del loro nome.

4.2 Permutazioni

4.2.1 Permutazioni semplici

Dati n elementi distinti, sono dette *permutazioni* di tali elementi tutti i possibili riordinamenti degli stessi. Un ragionamento molto semplice per visualizzare questo concetto è rivedere il problema come: “in quanti modi possibili possiamo mettere n oggetti in n posti?” Naturalmente ci saranno n scelte possibili per il primo posto, $n - 1$ per il secondo perché un oggetto è già stato scelto, $n - 2$ per il terzo e così via fino all’ultimo; ne consegue che il numero delle permutazioni $P(n)$ di n elementi è uguale al prodotto dei primi n numeri interi, cioè $n!$. Quindi:

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

Marco deve riordinare la sua stanza e deve, per ogni cassetto, mettere una camicia. Sapendo che i cassetti sono 4 come le camicie e che quest’ultime sono tutte di colori diversi, in quanti modi differenti Marco può riempire i cassetti?

La risposta è ovviamente $4!$, perché nel primo cassetto ci sono 4 scelte possibili, per ognuna di esse ci sono 3 scelte possibili per il secondo, 2 per il terzo e 1 sola per il quarto. Ho quindi, in totale $4 \cdot 3 \cdot 2 \cdot 1 = 4!$

4.2.2 Permutazioni con ripetizione

Se alcuni elementi da permutare sono uguali fra loro e indistinguibili, alcune permutazioni risulteranno identiche e dunque il numero complessivo sarà minore di $n!$. In questo caso, il numero di permutazioni di n oggetti di cui k_1 uguali a uno stesso oggetto a_1 , k_2 uguali a uno stesso oggetto a_2 , ..., k_m uguali ad uno stesso oggetto a_m , è dato dalla formula:

$$P(n) = \frac{n!}{k_1! \cdot k_2! \cdot \dots \cdot k_m!}$$

Calcolare il numero degli anagrammi della parola AMMETTERE.

Dobbiamo calcolare il numero delle permutazioni di 9 oggetti, di cui 3 uguali alla lettera E, 2 uguali alla lettera M, 2 uguali alla lettera T, 1 uguale alla lettera A e 1 alla lettera R; il numero di tali anagrammi è perciò:

$$P(n) = \frac{9!}{3! \cdot 2! \cdot 2!} = 15120$$

4.3 Disposizioni

4.3.1 Disposizioni semplici

Dati n elementi distinti e un numero $k \leq n$, le *disposizioni semplici* a k a k sono tutti i raggruppamenti che si possono formare con gli elementi dati, in modo che qualsiasi raggruppamento ne contenga k tutti distinti tra loro e che due raggruppamenti differiscano tra loro per qualche elemento oppure per l'ordine secondo il quale gli elementi si susseguono. Per visualizzare il concetto di disposizione, si pensi al problema come: "in quanti modi possibili possiamo mettere n oggetti in k posti ordinati?" Avremo quindi n scelte per il primo posto, $n-1$ per il secondo, $n-2$ per il terzo e così via fino al k -esimo posto, dove avremo $n-k+1$ possibili scelte da effettuare. Risulta quindi che il numero di tutte le possibili disposizioni $D_{n,k}$ di k elementi scelti tra n è:

$$D_{n,k} = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-(k+1)) = \frac{n!}{(n-k)!}$$

Nell'ippica, è denominata "corsa tris" una corsa in cui gli scommettitori devono indovinare i cavalli che arriveranno al primo, al secondo e al terzo posto. Supponendo che partano 10 cavalli, quanti sono le possibili scommesse?

Il problema si riduce al calcolo del numero di modi diversi in cui si possono disporre in ordine 3 cavalli in un insieme di 10. Tale numero è perciò $D_{10,3} = 10 \cdot 9 \cdot 8 = 720$.

Ricordiamo per concludere, questa utile relazione di cui non riportiamo la semplice dimostrazione: $(D_{n,k}) \cdot (D_{n-k,h}) = (D_{n,k+h})$.

4.3.2 Disposizioni con ripetizione

Dati n elementi diversi, le *disposizioni con ripetizione* di classe k sono tutti i raggruppamenti che si possono formare con gli elementi dati, in modo che ogni gruppo ne contenga k , ma ogni elemento possa trovarsi ripetuto nel gruppo un qualunque numero di volte e ogni gruppo differisca dall'altro per qualche elemento o per l'ordine con cui gli elementi sono disposti.

Quante colonne occorrerebbe giocare al totocalcio per essere certi di fare 13?

La risoluzione di questo problema non è un calcolo di disposizioni come sembrerebbe: infatti, ogni simbolo del totocalcio (1,2,X) può uscire più di una volta differentemente dalla definizione di disposizione. In questo caso, avremo 3 possibilità per il primo elemento della colonna, 3 per il secondo, 3 per il terzo e così via fino al tredicesimo. In totale bisognerà quindi giocare 3^{13} schedine, cioè 1.594.323.

Generalizziamo ora il problema: dobbiamo scoprire il numero di possibili modi in cui si possono scegliere n elementi a k a k sapendo che ogni elemento può essere ripetuto più di una volta. Allora avremo n possibilità per il primo elemento scelto, n per il secondo (poiché ogni elemento può essere ripetuto), n per il terzo e così fino al k -esimo. Risulta quindi che il numero di tutte le possibili disposizioni di k elementi scelti tra n con ripetizione $D'_{n,k}$ è:

$$D'_{n,k} = n^k$$

4.4 Combinazioni

4.4.1 Combinazioni semplici

Le *combinazioni* di n elementi a k a k ($k \leq n$) sono tutti i sottoinsiemi di k elementi di un dato insieme di n elementi, tutti distinti tra loro. La definizione appare molto simile a quella delle disposizioni, ma è importante capirne la differenza: le disposizioni differiscono per la presenza di elementi diversi o per l'ordine degli elementi, le combinazioni unicamente per la presenza di elementi diversi. Un tipico esempio di combinazione è un'estrazione a premi.

In quanti modi diversi è possibile estrarre i 5 numeri del lotto (i numeri sono compresi tra l'1 e il 90)?

In questo caso non importa affatto l'ordine con cui escono i numeri per la vincita e non si tratta quindi di una disposizione, dove invece c'è una prima uscita, una seconda uscita, ecc. Si tratta quindi di una combinazione di 90 elementi a 5 a 5.

Ragionando sulla definizione, risulta quasi naturale ottenere la formula delle combinazioni a partire dalle formule già note: infatti per ogni combinazione ci sono un numero di disposizioni pari alle permutazioni dei k elementi di cui la combinazione è formata (poiché l'ordine è ininfluenza, per esempio $\{1, 2, 3, 4, 5\}$ e la sua permutazione $\{2, 1, 3, 5, 4\}$ vengono contate una volta sola). La formula risulta quindi:

$$C_{n,k} = D_{n,k} / P_k = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

In una classe di 24 alunni si devono eleggere i 2 rappresentanti di classe. In quanti modi diversi si può fare questa scelta?

Poiché l'ordine di estrazione non è importante, si tratta di una combinazione di classe 2 di un insieme di 24 elementi; per cui, il numero delle scelte possibili è:

$$C_{24,2} = \frac{24!}{2! \cdot 22!} = 276$$

Soluzione problema di inizio capitolo.

Questa è la formula che permette anche di risolvere il problema, che ha introdotto il capitolo, del calcolo della probabilità di fare sei al SuperEnalotto: le sestine possibili sono $\binom{90}{6}$, il caso favorevole è naturalmente uno soltanto, per cui la probabilità richiesta è di:

$$\frac{1}{\binom{90}{6}} = \frac{1}{622.614.630}$$

4.4.2 Combinazioni con ripetizione

Le *combinazioni con ripetizione* di n oggetti di classe k sono i raggruppamenti che si possono formare scegliendo k elementi tra gli n di un insieme dato, ma ammettendo che ogni elemento possa trovarsi ripetuto nel gruppo un qualunque numero di volte: in questo modo ogni gruppo differirà dall'altro per almeno un elemento (o per quante volte è presente un elemento). Per visualizzare la cosa in un modo alternativo, a ogni elemento i vogliamo associare il numero di volte che esso è presente r_i , facendo in modo che $r_1 + r_2 + \dots + r_n = k$ (cioè il totale degli elementi sia k). Il numero di tali raggruppamenti è espresso dalla formula:

$$C'_{n,k} = \frac{(n+k-1)!}{k!(n-1)!} = \binom{n+k-1}{k}$$

Questa formula può essere dimostrata sfruttando l'ultima relazione segnata, in modo simile all'esercizio 5 a pagina 70.

Qual è il numero massimo di termini che può comparire in un polinomio omogeneo di terzo grado nelle 4 variabili x, y, z, t ?

Risulta ovvio che ciascuno dei polinomi che considereremo non dovrà contenere termini simili. La parte di ogni termine di tale polinomio può essere associata a una combinazione con ripetizione di classe 3 degli elementi dell'insieme costituito dalle 4 variabili: l'esponente di ciascuna lettera indicherà il numero di volte che questa si ripete; ad esempio il termine y^2t sarà associato alla combinazione yyt ; x^3 sarà associato alla combinazione xxx , e così via. Il numero massimo di termini che il polinomio può contenere sarà quindi dato dal numero di combinazioni con ripetizione di classe 3 di 4 oggetti, ossia

$$C'_{4,3} = \binom{4+3-1}{3} = \binom{6}{3}$$

4.5 Principio di inclusione-esclusione

Dato un insieme M , la sua *cardinalità* $|M|$ è definita come il numero di elementi che lo compongono. Preso per esempio l'insieme $S = \{a, b, c, d\}$, la sua cardinalità $|S|$ è 4. Il principio di inclusione-esclusione è una tecnica di conteggio che permette di calcolare la cardinalità di un'unione di insiemi in funzione della cardinalità degli insiemi e delle intersezioni degli stessi. Questo principio generalizza al caso di n insiemi la nota relazione $|A \cup B| = |A| + |B| - |A \cap B|$: per avere la cardinalità dell'unione di più insiemi, dobbiamo sommare la cardinalità di ciascuno degli insiemi, sottrarre le cardinalità di tutte le possibili intersezioni a 2 a 2 (che sono state contate due volte), riaggiungere le cardinalità di tutte le possibili intersezioni a 3 a 3 (che sono state sottratte una volta di troppo), e così via. In formule:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{i=1}^n |A_i| - \sum_{i < j} |A_i \cap A_j| + \sum_{i < j < k} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$

Se ad esempio vogliamo applicarlo all'unione di 3 insiemi abbiamo che $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$. Notiamo che arrestandosi in un qualsiasi punto della somma, si ottiene una maggiorazione se il primo termine trascurato ha segno negativo, o una minorazione se il primo termine trascurato ha segno positivo.

Quanti sono i numeri non coprimi con 30 da 1 a 100?

Quest'esercizio, in apparenza complesso, è in realtà una semplice applicazione del principio di inclusione-esclusione. Infatti i numeri non coprimi con 30 sono quelli multipli o di 2, o di 3 o di 5; per cui se si definiscono $A = \{\text{multipli di 2}\}$, $B = \{\text{multipli di 3}\}$ e $C = \{\text{multipli di 5}\}$, allora il problema diventa contare gli elementi dell'unione fra i tre insiemi e quindi sottrarre gli elementi che appartengono alle 3 intersezioni a due a due e sommare gli elementi appartenenti all'intersezione comune a tutti. Gli insiemi citati corrispondono a: $A \cap B = \{\text{multipli di 6 da 1 a 100}\}$, $A \cap C = \{\text{multipli di 10 da 1 a 100}\}$, $B \cap C = \{\text{multipli di 15 da 1 a 100}\}$ e $A \cap B \cap C = \{\text{multipli di 30 da 1 a 100}\}$. A questo punto basta trovare le cardinalità, che risultano $|A| = 50$, $|B| = 33$, $|C| = 20$, $|A \cap B| = 16$, $|A \cap C| = 10$, $|B \cap C| = 6$ e $|A \cap B \cap C| = 3$. E quindi: $|A \cup B \cup C| = 33 + 50 + 20 - 16 - 6 - 10 + 3 = 74$.

4.6 Conteggi classici

Come conclusione del capitolo di combinatoria, ricordiamo alcune formule che possono essere molto utili per la risoluzione di alcuni esercizi presenti nelle olimpiadi di matematica.

- La somma dei primi n numeri naturali è data dalla formula

$$\frac{n \cdot (n + 1)}{2}$$

- La somma dei primi n quadrati è data dalla formula

$$\frac{n \cdot (n + 1) \cdot (2n + 1)}{6}$$

- La somma dei primi n cubi è data dalla formula

$$\frac{n^2 \cdot (n + 1)^2}{4}$$

- Il numero delle diagonali di un poligono di n vertici è dato dalla formula:

$$D = \frac{n \cdot (n - 3)}{2}$$

Infatti ogni vertice può essere collegato agli $n - 3$ vertici non adiacenti (tutti i vertici tranne se stesso, quello alla sua destra, e quello alla sua sinistra). In questo modo, tuttavia, ogni diagonale $A_i A_j$ viene contata due volte: una volta come uscente da A_i e una volta come uscente da A_j . Occorre quindi dimezzare, ottenendo la formula cercata.

- Dati due insiemi A e B , viene definito *prodotto cartesiano* l'insieme chiamato $A \times B$ e costituito da tutti gli elementi del tipo (a, b) con $a \in A$ e $b \in B$. In formule:

$$A \times B = \{(a, b) / a \in A, b \in B\}$$

Per esempio, dati gli insiemi $A = \{1, 2\}$ e $B = \{3, 4\}$, l'insieme prodotto cartesiano è $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$. La cardinalità dell'insieme $|A \times B|$ è ovviamente uguale al prodotto delle due cardinalità:

$$|A \times B| = |A| \cdot |B|$$

- Dato un insieme S , viene definito *insieme delle parti* di S , scritto $\wp(S)$, l'insieme di tutti i possibili sottoinsiemi di S compreso l'insieme vuoto e l'insieme S stesso. Sia $M = \{1, 2, 3\}$, allora $\wp(M) = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}, \{2\}, \{3\}, \emptyset\}$. La cardinalità dell'insieme delle parti è:

$$|\wp(A)| = 2^{|A|}$$

Infatti, fare la cardinalità dell'insieme delle parti consiste nel sommare tutti i possibili sottoinsiemi di un insieme e quindi sommare tutte le possibili combinazioni dei suoi elementi (si veda la definizione di combinazione), cioè $\sum_{k=0}^n \binom{n}{k}$ che, dal paragrafo introduttivo, sappiamo essere uguale a 2^n .

- Si consideri il numero m con scomposizione in fattori primi $m = p^\alpha$: risulta ovvio che m avrà come unici divisori $1, p, p^2, p^3, \dots, p^\alpha$. Il numero di tali divisori è dunque $\alpha + 1$. Se invece consideriamo un numero m' con scomposizione in fattori $m' = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$, rifacendosi al procedimento precedente otteniamo che il numero di divisori di m' è $(\alpha_1 + 1) \cdot (\alpha_2 + 1)$: infatti ogni divisore sarà del tipo $d = p_1^{\beta_1} \cdot p_2^{\beta_2}$ con $0 \leq \beta_i \leq \alpha_i$, e possiamo scegliere β_1 in $(\alpha_1 + 1)$ modi e β_2 in altri $(\alpha_2 + 1)$ modi indipendenti. Sia infine $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ la fattorizzazione in numeri primi di n qualunque. Se si utilizza un ragionamento analogo a quello condotto sopra, si ottiene che il numero di divisori di n è dato da:

$$(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_k + 1)$$

Cerchiamo ora di capire come si può esprimere in formula la somma dei divisori di un numero. Consideriamo nuovamente il numero $m = p^\alpha$: la somma dei suoi divisori sarà data dall'espressione $(1 + p + p^2 + p^3 + \dots + p^\alpha)$. In modo analogo si ottiene la formula generale:

$$\begin{aligned} & (1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1}) \cdot (1 + p_2 + p_2^2 + \dots + p_2^{\alpha_2}) \cdot \dots \cdot (1 + p_k + p_k^2 + \dots + p_k^{\alpha_k}) = \\ & = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \end{aligned}$$

Infatti, distribuendo i prodotti nella prima formula precedente, si ottiene la somma di tutti i possibili fattori $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k}$.

- Dati due interi, n non negativo, e k positivo, definiamo una *partizione* dell'intero n in k parti, una scrittura di n come $n_1 + n_2 + \dots + n_k$, dove i vari n_i sono non negativi. Il numero totale delle partizioni di un intero, tenendo conto dell'ordine con cui viene partizionato

(per esempio, $12 = 3 + 5 + 4$ è diverso da $12 = 5 + 3 + 4$), è dato da:

$$\binom{n+k-1}{k-1}$$

Un esempio a tal proposito è dato nel già citato all'esercizio 5 a pagina 70, e la dimostrazione generale segue la falsariga di tale esempio.

4.7 Probabilità

4.7.1 Definizione

Nello studio degli esperimenti casuali la *probabilità* di un evento è, intuitivamente, un numero compreso tra 0 e 1 che rappresenta quanto questo sia “possibile” (o ancor meglio, “probabile”). Lo 0 corrisponde a un evento impossibile, mentre l'1 corrisponde a un evento certo.

Per poter misurare matematicamente le probabilità occorre definire uno *spazio campione*, cioè l'insieme di tutti i possibili esiti dell'esperimento casuale che ci interessa (esiti incompatibili fra loro: il verificarsi di uno di essi esclude il verificarsi degli altri). Per esempio, nel lancio di un dado a 6 facce lo spazio campione è l'insieme $S = \{1, 2, 3, 4, 5, 6\}$.

Gli *eventi* vengono rappresentati come sottoinsiemi dello spazio campione: in termini non matematici un evento equivale a dire “accade uno dei miei elementi”, e gli elementi appartenenti all'evento sono detti *casi favorevoli* all'evento. Per esempio, nel caso di prima un evento è $E = \{1, 3\}$, $E \subseteq S$, e significa “esce 1 oppure esce 3”. Un evento si dice *elementare* se contiene un solo elemento, si dice *evento certo* se coincide con l'insieme campione, o *evento impossibile* se è l'insieme vuoto.

Consideriamo un dado a 4 facce bilanciato. Lo spazio degli eventi è $S = \{1, 2, 3, 4\}$; l'evento certo è lo stesso S (“esce un qualunque numero”); un evento elementare è, per esempio, $A = \{2\}$ (“esce 2”), mentre un evento qualsiasi è $B = \{2, 4\}$ (“esce 2 o esce 4”, analogamente “esce un numero pari”).

Quando si pensa a un evento, in modo intuitivo, si pensa certamente a una qualche frase \mathcal{P} che lo descrive: per esempio, proprio “esce un numero pari”. Perché allora non utilizzare questa definizione anche in matematica? Questa definizione intuitiva, inoltre, ha certamente il pregio di rendere quasi ovvie le composizioni tra eventi: se per esempio consideriamo due eventi \mathcal{P} e \mathcal{Q} , diventa immediato definire gli eventi “ \mathcal{P} oppure \mathcal{Q} ” (accade almeno uno dei due), “ \mathcal{P} e \mathcal{Q} ” (accadono entrambi), e così via.

Da un punto di vista matematico, tuttavia, questa definizione seppure più intuitiva sarebbe risultata molto più scomoda: come è possibile, infatti, calcolare un numero (la probabilità) a partire da una proposizione? Di certo è arduo basarsi sulla struttura della frase. Avendo invece definito gli eventi come insiemi questo calcolo è quasi immediato: in uno spazio campione S , la probabilità $P(E)$ dell'evento E è data da

$$P(E) = \frac{|E|}{|S|}$$

In altre parole, la probabilità di un evento è il rapporto tra la cardinalità dell'evento (il numero di casi favorevoli) e la cardinalità dello spazio campione (il numero di casi possibili). Chiaramente si presuppone che tutti i casi possibili (gli elementi di S) siano equiprobabili.

In verità, la rappresentazione per insiemi è particolarmente comoda perché è anche immediata la definizione di eventi composti, così come tra le proposizioni: sia infatti A l'evento corrispondente ad "accade \mathcal{P} " e B l'evento corrispondente ad "accade \mathcal{Q} ". Non è difficile verificare che l'evento $A \cup B$ corrisponde ad "accade \mathcal{P} o \mathcal{Q} ", l'evento $A \cap B$ ad "accadono \mathcal{P} e \mathcal{Q} ", e l'evento $\bar{A} = S \setminus A$ corrisponde a "non accade \mathcal{P} ". Usando gli eventi introdotti nell'esempio precedente, il complementare di A è $\bar{A} = \{1, 3, 4\}$ ("non esce 2"), l'unione $A \cup B = \{2, 4\}$ mentre l'intersezione è $D = \{2\}$.

Calcola la probabilità che, lanciando un dado, esca un numero pari.

Lo spazio campione è ovviamente $S = \{1, 2, 3, 4, 5, 6\}$, mentre l'evento considerato è $E = \{2, 4, 6\}$ e contiene tre elementi, ossia 3 sono i casi favorevoli. Dunque:

$$P(E) = \frac{|E|}{|S|} = \frac{3}{6} = \frac{1}{2}$$

Osserviamo che il calcolo di probabilità si riconduce al calcolo di cardinalità di insiemi; che è in pratica l'argomento affrontato nei paragrafi precedenti. Infatti il calcolo delle probabilità è proprio l'applicazione principale del calcolo combinatorio.

Da un'urna contenente 6 palline bianche e 9 blu, se ne estraggono 2 contemporaneamente. Calcolare la probabilità degli eventi:

$A =$ "le palline estratte sono entrambe bianche"

$B =$ "le palline estratte sono una blu e una bianca"

I casi possibili sono tutti i gruppi di 2 palline che si possono estrarre dall'urna, ossia i sottoinsiemi di due elementi dell'insieme delle 15 palline contenute nell'urna. Il loro numero è dunque quello delle combinazioni di 15 oggetti a 2 a 2:

$$|S| = C_{15,2} = \binom{15}{2} = 105$$

I casi favorevoli dell'evento A corrispondono ai gruppi di due palline bianche che si possono formare, ossia i sottoinsiemi di due elementi dell'insieme delle 6 palline bianche. Il loro numero è dunque quello delle combinazioni di 6 oggetti a 2 a 2:

$$|A| = C_{6,2} = \binom{6}{2} = 15$$

La probabilità dell'evento A è dunque:

$$P(A) = \frac{|A|}{|S|} = \frac{15}{105} = \frac{1}{7}$$

I casi favorevoli dell'evento B corrispondono ai gruppi costituiti da una pallina bianca e una blu; ciascuno di tali gruppi si ottiene associando, a una delle 6 palline bianche, una delle 9 palline blu. Tali gruppi sono quindi in numero di

$$|B| = 6 \cdot 9 = 54$$

La probabilità dell'evento B è dunque:

$$P(B) = \frac{|B|}{|S|} = \frac{54}{105} = \frac{18}{35}$$

4.7.2 Probabilità di eventi composti

Dati due eventi A e B , questi si dicono *incompatibili* se non si possono verificare contemporaneamente, cioè se e solo se la loro intersezione è l'evento impossibile. Una corretta traduzione in campo insiemistico è affermare che la loro intersezione $A \cap B = \emptyset$.

Due eventi C e D si dicono invece *compatibili* se si possono verificare contemporaneamente; ne consegue naturalmente che $A \cap B \neq \emptyset$.

Se io tiro due volte un dado, gli eventi $A = \{\text{esce un numero pari}\}$ e l'evento $B = \{\text{esce } 1\}$, sono compatibili o incompatibili?

Gli eventi sono chiaramente incompatibili, infatti $A \cap B = \emptyset$.

Se io tiro due volte un dado, gli eventi $C = \{\text{esce un numero pari}\}$ e l'evento $D = \{\text{esce un numero primo}\}$, sono compatibili?

Sì, gli eventi sono compatibili. Questo perché l'intersezione è diversa dall'insieme vuoto, infatti $A \cap B = \{\text{esce } 2\}$.

Vedremo ora come si può esprimere la probabilità di eventi composti. Dato un evento A e il suo complementare \bar{A} , fra le due probabilità vale la relazione:

$$P(A) = 1 - P(\bar{A})$$

La formula che in generale esprime la probabilità dell'unione di due eventi è invece:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Naturalmente risulta che se due eventi sono incompatibili allora, dato che la probabilità dell'intersezione è l'insieme vuoto:

$$P(A \cup B) = P(A) + P(B)$$

Si noti che questa formula è una naturale applicazione del principio di inclusione ed esclusione.

Calcola la probabilità che il primo numero del lotto estratto sulla ruota di Napoli sia un numero dispari o un multiplo di 18.

L'evento di cui si chiede la probabilità è l'unione dei due eventi seguenti: A = "il primo estratto è un numero dispari", B = "il primo estratto è un multiplo di 18". I due eventi sono evidentemente incompatibili e dunque posso utilizzare la formula $P(A \cup B) = P(A) + P(B)$. Per entrambi gli eventi i casi possibili sono 90; per l'evento A i casi favorevoli sono 45, mentre per l'evento B notiamo che ci sono solo 5 multipli di 18 compresi tra 1 e 90. Risulta quindi:

$$P(A) = \frac{45}{90}$$

$$P(B) = \frac{5}{90}$$

E quindi:

$$P(A \cup B) = P(A) + P(B) = \frac{45}{90} + \frac{5}{90} = \frac{5}{9}$$

4.7.3 Probabilità condizionata e dell'intersezione

Si definisce come *probabilità condizionata* la probabilità che si sia verificato A sapendo che si è già verificato B : questa è uguale al rapporto tra la probabilità che si verifichino sia A che B è la probabilità che si verifichi B . Si tratta quindi di una sorta di "correzione" delle aspettative dettata dall'osservazione di B . In formule:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Un esempio banale di probabilità condizionata è estrarre per due volte consecutive una pallina nera da un cesto con 5 palline nere e 5 bianche: ovviamente la probabilità di estrazione di una seconda pallina nera è soggetta al risultato della prima estrazione. Nel caso due eventi siano incompatibili, allora la probabilità di B dato A è semplicemente uguale alla probabilità di B poiché non si possono verificare contemporaneamente. Usando quest'ultima definizione, possiamo introdurre la probabilità dell'intersezione di due eventi:

$$P(A \cap B) = P(A) \cdot P(B|A)$$

cioè la probabilità che si verifichi A dato B è la probabilità dell'intersezione di A con B diviso la probabilità di B . Nel caso due eventi siano indipendenti, la formula diventa:

$$P(A \cap B) = P(A) \cdot P(B)$$

Da un'urna contenente 3 palline rosse e 5 blu, se ne estraggono 2, senza reinserire la prima pallina estratta prima di procedere alla seconda estrazione. Calcola la probabilità di estrarre due palline blu.

Prendiamo in considerazione i seguenti eventi: $A = \{\text{la prima pallina estratta è blu}\}$,

$B = \{\text{la seconda pallina estratta è blu}\}$. Si calcoli la probabilità dell'evento $A \cap B$. A e B sono evidentemente compatibili per cui utilizziamo la formula: $P(A \cap B) = P(A) \cdot P(B|A)$. Bisogna quindi prima calcolare $P(A)$ e $P(B|A)$. Per calcolare $P(A)$, consideriamo che vi sono 8 esiti ugualmente possibili, uno per ciascuna pallina contenuta nell'urna, e di questi 5 sono favorevoli, dunque è:

$$P(A) = \frac{5}{8}$$

Se si verifica A nell'urna rimangono 7 palline di cui 4 blu e quindi è:

$$P(B|A) = \frac{4}{7}$$

Si ha perciò:

$$P(A \cap B) = P(A) \cdot P(B|A) = \frac{5}{8} \cdot \frac{4}{7} = \frac{5}{14}$$

4.8 Approfondimenti

4.8.1 Valor medio

Sia X una *variabile aleatoria*, ovvero una funzione che associa ad ogni evento un numero reale. Per esempio, se dobbiamo contare il numero di volte che esce testa dal lancio di una moneta, la variabile aleatoria riferita al singolo lancio può assumere il valore 1 se esce testa (e dunque con probabilità $\frac{1}{2}$), mentre il valore 0 se esce croce (quindi con la stessa probabilità). Oppure, considerando il lancio di un dado, si può associare l'evento esce il numero n al valore n di una variabile aleatoria, che nel caso tradizionale di un dado a sei facce sarà di conseguenza un intero compreso tra 1 e 6 (estremi inclusi), con probabilità che ognuno venga assunto di $\frac{1}{6}$.

Siano ora x_1, x_2, \dots, x_n i valori che può assumere la variabile aleatoria, e siano p_1, p_2, \dots, p_n le rispettive probabilità. Definiamo il *valor medio* di una variabile aleatoria, e lo indichiamo con la scrittura $\mathbb{E}(X)$, la quantità:

$$\mathbb{E}(X) = p_1 x_1 + p_2 x_2 + \dots + p_n x_n = \sum_{i=1}^n p_i x_i$$

Considerando i due esempi precedenti, siano X_M la variabile aleatoria con riferimento al caso del lancio della moneta, e X_D quella con riferimento al lancio del dado. Allora:

$$\mathbb{E}(X_M) = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot 1 = \frac{1}{2} = 0.5$$

$$\mathbb{E}(X_D) = \frac{1}{6} \cdot 1 + \frac{1}{6} \cdot 2 + \frac{1}{6} \cdot 3 + \frac{1}{6} \cdot 4 + \frac{1}{6} \cdot 5 + \frac{1}{6} \cdot 6 = \frac{1}{6} \cdot 21 = \frac{7}{2} = 3.5$$

Il valor medio gode delle seguenti proprietà:

- linearità:
 - il valor medio della somma è uguale alla somma dei valori medi; in simboli:

$$\mathbb{E}(X + Y) = \mathbb{E}(X) + \mathbb{E}(Y)$$
 - il valor medio di una v.a. moltiplicata per una costante è uguale alla costante per il valor medio; in simboli:

$$\mathbb{E}(c \cdot X) = c \cdot \mathbb{E}(X)$$

- combinando i due risultati precedenti, si ottiene la definizione classica di linearità, equivalente alle due sopra date:

$$\mathbb{E}(a \cdot X + b \cdot Y) = a \cdot \mathbb{E}(X) + b \cdot \mathbb{E}(Y)$$

- positività: il valor medio di una v.a. definita positiva, ovvero tale da assumere soltanto valori positivi o nulli, è anch'esso positivo o nullo. In simboli:

$$X \geq 0 \implies \mathbb{E}(X) \geq 0$$

- convessità: il valor medio di una v.a. è *compreso* tra il più piccolo e il più grande valore che essa può assumere, e più nello specifico è *strettamente compreso* se i due non coincidono. Si noti che la proprietà di positività può essere vista come un caso particolare della convessità, dove gli estremi sono entrambi maggiori o uguali a 0 e pertanto lo è anche la media che ne è compresa.

- moltiplicatività in caso di indipendenza: se due v.a. sono indipendenti, ovvero (informalmente) il risultato di una non influenza l'altra, nel senso che si riferiscono a procedimenti che non c'entrano l'uno con l'altro, come possono essere per esempio il lancio di due monete distinte o il lancio di due dadi distinti (non invece il lancio di un dado e la somma del lancio dello stesso dado con un altro), vale anche che il valor medio del loro prodotto è uguale al prodotto dei loro valori medi. In simboli:

$$\mathbb{E}(X \cdot Y) = \mathbb{E}(X) \cdot \mathbb{E}(Y)$$

Il risultato non vale invece, in generale, se si considerano due v.a. dipendenti, ovvero tali per cui il risultato di una influenza l'altra.

4.8.2 Periodo di una permutazione

Una permutazione può essere considerata come un modo di riarrangiare una fila di oggetti numerati in ordine. Ad esempio, partendo da 12345 possiamo ottenere 35124: se esaminiamo la struttura di questa permutazione, osserviamo che essa è ottenuta scambiando gli oggetti al primo e terzo posto e permutando ciclicamente gli oggetti ai posti 2, 5 e 4. Questa azione di scambio di posti può essere iterata nuovamente: a partire da 35124, scambiando il primo e il terzo posto si ha 15324, e permutando ciclicamente i posti 2, 5 e 4 si arriva a 14352. Continuando ad applicare questa sequenza di operazioni si ottiene questa lista:

12345

35124

14352

32145

15324

34152

12345

La sesta volta si ottiene di nuovo l'ordine iniziale. In generale, il *periodo* di una permutazione è il numero minimo di volte che è necessario applicare una permutazione affinché si ritorni alla configurazione iniziale. Esiste un modo rapido per calcolare il periodo di una permutazione, che illustreremo in questo paragrafo.

Cominciamo con il fissare una notazione utile: una scrittura del tipo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

significa che il primo posto è occupato dall'oggetto numero 3, il secondo dal numero 5 e così via. Se consideriamo il numero 1 nella prima riga, la notazione ci dice che esso viene mandato al terzo posto. Se ora guardiamo il numero 3 nella prima riga vediamo che è spostato al primo posto. Nella successione delle permutazioni pertanto al primo posto si alternano 1 e 3, e al terzo posto 3 e 1. Un fenomeno analogo succede per i posti 2, 5 e 4. Si è soliti usare una scrittura del tipo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = (13)(254)$$

Prendiamo in esame quello che accade ai posti 1 e 3: applicando un numero pari di volte la permutazione, si ritrova la configurazione iniziale. Nei posti 2, 5 e 4 invece la situazione iniziale si ritrova ogni 3 volte. Ne segue che per ottenere di nuovo la successione 12345 è necessario applicare la permutazione (13)(254) per 6 volte.

In generale, una volta scritta la permutazione nella forma

$$(a_1 \dots a_n)(b_1 \dots b_m) \dots (c_1 \dots c_q)$$

il suo periodo è il minimo comune multiplo dei numeri $n, m \dots q$

Consideriamo la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

Come scriverla nella forma indicata sopra?

Vediamo che cosa fa l'oggetto 1 applicandola ripetutamente: esso va nel posto 5, poi di nuovo nel posto 1, e analogamente per i posti 5 e 6. Ne segue che possiamo scrivere la permutazione come (15)(24) e pertanto il suo periodo è 2. Invece il periodo di

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}$$

è 4. Infatti, l'oggetto 1 va nel posto 2, e poi (nell'ordine) nei posti 3 e 4, per poi tornare nella sua posizione iniziale. L'oggetto 5 invece va nel posto 6 e poi di nuovo nel posto 5: possiamo quindi scrivere la permutazione come (1234)(56).

4.9 Esercizi

4.9.1 Esercizi di base

Combinatoria

1. 12 persone si stringono la mano, ciascuna stringe la mano a tutte le altre. Quante sono le strette di mano in totale?
2. Un cartolaio ha nel suo negozio tre cassetti liberi; vuole sistemare in tali cassetti le biro nere, blu e rosse, suddivise secondo i colori. In quanti modi diversi può disporre le penne nei cassetti?
3. Quanti numeri di 9 cifre tutte diverse tra loro (e diverse da 0) si possono scrivere?
4. In quanti modi diversi possiamo disporre 4 bottiglie di vino rosso, tra loro identiche, e 6 bottiglie di vino bianco, anch'esse identiche, in uno scaffale con 10 scomparti? E se gli scomparti sono 12?
5. Un sistemista del totocalcio vuole giocare tutte le possibili colonne in cui figurano sei segni 1, cinque segni X e due segni 2. Inoltre, sa che nelle colonne da giocare vi sono tre fisse: nella prima e nell'ottava partita sia fisso il segno 1, nella quinta partita il segno X. Quante colonne dovrà giocare?
6. Le disposizioni di un certo numero di oggetti a 5 a 5 sono tante quante sono le disposizioni degli stessi oggetti a 4 a 4. Determina il numero degli oggetti.
7. Tra tutti i numeri di 6 cifre, tutte diverse tra loro, quante sono quelli le cui prime tre cifre sono dispari e le restanti pari?
8. Quanti sono i numeri di 6 cifre di cui le prime tre dispari e le restanti pari?
9. Le nuove targhe automobilistiche sono costruite da 2 lettere, seguite da 3 cifre, seguite a loro volta da 2 lettere. Sapendo che le lettere possono essere scelte tra le 26 dell'alfabeto anglosassone, calcola quante automobili si possono immatricolare in questo modo?
10. Si mescolano 10 carte e se ne distribuiscono 5 al giocatore A e 5 al giocatore B. In quanti modi diversi può avvenire la distribuzione?
11. In una classe di 20 studenti si devono formare una squadra di calcio e una di pallacanestro. In quanto modi diversi si possono formare le due squadre, se nessuno studente

può appartenere a entrambe?

12. Si lanciano 4 dadi identici. Quante combinazioni si possono formare?
13. Quattro giocatori si affrontano in una partita a carte. Sapendo che il numero complessivo di punti in palio è 11, si calcoli il numero dei possibili esiti della partita.
14. Sviluppare le potenze:

$$(a + b)^7, (x + y)^8$$

15. Calcolare il numero dei lati di un poligono convesso avente 90 diagonali.
16. Dimostrare che le diagonali di un poligono convesso di n lati si intersecano in $\binom{n}{4}$ punti interni al poligono.
17. Tre paia di calzini, uno rosso, uno blu e uno verde, sono stesi in fila. Sapendo che due calzini dello stesso colore non sono vicini uno all'altro, quante successioni di colori si possono avere?
18. Determinare il periodo delle permutazioni

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}$$

e

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 1 & 4 & 5 \end{pmatrix}$$

19. Sono state istituite tre commissioni parlamentari formate da 10 membri ciascuna. Sapendo che nessun parlamentare è membro simultaneamente di tutte e tre le commissioni, qual è il numero minimo di persone coinvolte?
20. Un poligono regolare ha n lati e $4n$ diagonali. Calcolare n .
21. Avendo a disposizione cinque cifre uguali a 1 ed una cifra uguale a 2, quanti numeri diversi possono essere costruiti, senza avere il vincolo di utilizzare tutte le cifre (ovvero si possono utilizzarle tutte ma è possibile anche farne uso solamente di alcune?)
22. Calcolare $\binom{6}{0} + \binom{6}{1} + \binom{6}{2} + \binom{6}{3} + \binom{6}{4} + \binom{6}{5} + \binom{6}{6}$

Probabilità

23. Si lanciano due monete; da quanti eventi è costituito lo spazio degli eventi?
24. Si lanciano due dadi. Si calcoli prima la probabilità di ottenere due facce uguali, poi la probabilità che la somma dei punti faccia 6.
25. In un contenitore vi sono 100 matite di cui 12 difettose. Si scelgono a caso 4 matite; calcola la probabilità di estrarre 4 matite difettose.
26. Tre amici acquistano 3 biglietti per 3 posti contigui al cinema. Si siedono a caso. Calcolare la probabilità che il più piccolo sia seduto al centro, sapendo che le età sono tutte diverse fra loro.
27. Un sacchetto contiene 21 palline, su cui sono incise le lettere dell'alfabeto italiano. Si estraggono contemporaneamente 4 palline. Calcolare la probabilità di ottenere le lettere per formare la parola *moro*.
28. Considerato un gruppo di 5 persone, calcolare la probabilità che tutte abbiano il nome che inizia per la stessa lettera (considerando le 20 lettere dell'alfabeto), supponendo che le iniziali dei nomi siano tutte equiprobabili. Qual'è la probabilità che abbiano tutte e 5 le iniziali diverse?
29. Si estrae una carta da un mazzo di 40 carte. Qual'è la probabilità di estrarre una figura nell'ipotesi che sia stata estratta una carta di cuori?
30. Da un mazzo di 40 carte se ne estraggono 3 successivamente. Calcolare la probabilità che siano tutte e tre carte di fiori, sia nel caso che ciascuna carta estratta venga reinserita prima di procedere all'estrazione successiva, sia nel caso che le tre carte estratte non vengano reinserite.
31. In un astuccio vi sono 15 pennarelli, di cui 5 sono esauriti. Estrahendo a caso e successivamente, 3 pennarelli senza reintrodurli nell'astuccio, calcolare la probabilità che nessun pennarello sia esaurito.
32. Un'urna contiene 60 palline di cui 22 blu e 38 rosse. Si estraggono successivamente 3 palline senza rimettere le palline nell'urna. Calcolare la probabilità che si estraggano 2 palline blu e una rossa.

33. Un tale ha in tasca 6 monete: 2 da 200 lire, 2 da 100 lire, 2 da 50 lire. Egli vuole acquistare una cartolina da 300 lire, pesca a caso tre monete dalla sua tasca e le dà al negoziante. Calcola la probabilità p che il negoziante gli dia la cartolina
34. Tre amici possiedono ciascuno tre gettoni e giocano con un dado da tre. Dopo ogni partita il vincitore riceve un gettone da ognuno degli altri due amici. Qual è la probabilità che il gioco non si debba interrompere entro cinque partite poiché uno dei giocatori rimane senza gettoni?
35. Qual'è il numero minimo di carte che bisogna pescare da un ordinario mazzo da 52 carte per avere almeno il 50% di probabilità di estrarre una o più carte di cuori?
36. Gianni ha deciso che tira un dado a 6 facce e vince quando ottiene 5 o 6; ma se ottiene 1 può ritirare il dado e ripetere il procedimento. Qual è la probabilità di vittoria di Gianni?
37. In una lotteria vengono estratti, uno per volta, i numeri da 1 a 4 in un ordine qualsiasi. Qual è la probabilità che i primi tre numeri escano in ordine crescente?
38. Lanciati due dadi, qual è la probabilità che la somma delle dieci facce visibili sia divisibile per 35?
39. Un componente di un macchinario è libero di spostarsi su di una struttura a forma di griglia quadrata di dimensioni sufficientemente grandi con quadretti di lato 1 passo. A causa di un virus informatico che ha intaccato il suo sistema di controllo, ad un certo punto il componente, che si trova in posizione $(2, 1)$, inizia a muoversi, decidendo ad ogni vertice della griglia di prendere casualmente una direzione, ognuna con la stessa probabilità delle altre. Qual è la probabilità che, dopo 6 passi, si trovi al punto $(0, -3)$?

4.9.2 Esercizi svolti

Combinatoria

1. In quanti modi si possono disporre 3 ragazzi e 3 ragazze per una foto di gruppo, sistemando i ragazzi accovacciati e le ragazze in piedi dietro di loro?
(A) 9 (B) 24 (C) 36 (D) 54 (E) 81
2. Ho a disposizione cinque cifre uguali a 1 e una cifra uguale a 2. Usando tutte o alcune di queste cifre, quanti diversi numeri naturali posso costruire?
(A) 15 (B) 21 (C) 24 (D) 26 (E) 27
3. Dato un cubo C , quanti sono i triangoli che hanno per vertici tre vertici di C e non giacciono su nessuna delle facce di C ?
(A) 12 (B) 24 (C) 32 (D) 56 (E) 112
4. Due matematici, tre fisici e cinque ingegneri sono seduti in prima fila ad una conferenza. Dire in quanti modi si possono disporre per ognuno dei seguenti vincoli:

- se quelli dello stesso corso devono sedersi vicini?
 - se quelli dello stesso corso si considerano indistinguibili?
 - se possono mettersi dove vogliono e si considerano tutti diversi? E se un fisico e un ingegnere sono gemelli (quindi da considerarsi uguali)?
5. Quante sono le terne ordinate di interi non negativi tali che risulti $a + b + c = 57$?
6. Alessio ha un tavolo rotondo con sei sedie tutte di colori diversi. Si domanda quante sono le diverse disposizioni delle sedie attorno al tavolo (N.B.: due disposizioni si considerano uguali se è possibile ottenere una dall'altra mediante una rotazione).
7. Qual'è il più piccolo naturale con esattamente 15 divisori?
8. In quanti modi possiamo scegliere 3 sottoinsiemi A, B, C di $\mathcal{U} = \{1, 2, \dots, n\}$ in modo che $A \cap B \cap C = \emptyset$, $A \cap B \neq \emptyset$, $A \cap C \neq \emptyset$.

Probabilità

9. Oggi, come ogni sabato mattina, Francesco e Lorenzo si affrontano in una serie di partite a bowling. Vince chi si aggiudica per primo 5 partite. Inoltre, Francesco è consapevole che Lorenzo, avendo più esperienza, vince contro di lui con probabilità $4/7$.
- Qual è la probabilità che si arrivi a disputare la nona partita?
 - Qual è la probabilità che Francesco vinca alla settima partita?
10. Si consideri un mazzo da 40 carte. Matteo pesca 5 carte.
- Qual è la probabilità che abbia pescato esattamente tre assi?
 - Qual è la probabilità che, cambiando una delle due carte che non sono assi, ottenga il poker d'assi?
11. In un'urna ci sono 3 palline gialle, 2 rosse e 4 bianche.
- Calcolare il numero di possibili combinazioni di 5 palline di cui due gialle, una rossa e due bianche.
- Matteo estrae una pallina: se gialla la toglie e ne aggiunge una rossa; se rossa la reinserisce e ne aggiunge un'altra rossa; se bianca la toglie.
- Alla seconda estrazione, qual è la probabilità di estrarre una pallina bianca?
 - Qual è la probabilità che, avendo estratto una bianca alla seconda estrazione, alla prima estrazione fosse uscita una pallina gialla?
12. Quattro squadre di pallacanestro di pari forza disputano un torneo con girone unico all'italiana (ogni squadra incontra ogni altra squadra una sola volta). Qual è la probabilità che ci sia una squadra che alla fine del torneo ha vinto tutte le sue partite? (le partite di pallacanestro non possono finire con un pareggio).
- (A) $\frac{1}{6}$ (B) $\frac{1}{\pi}$ (C) $\frac{1}{3}$ (D) $\frac{1}{2}$ (E) $\frac{2}{3}$

13. Lanciati due dadi, qual è la probabilità che la somma delle dieci facce visibili sia divisibile per 35?
(A) $\frac{5}{36}$ (B) $\frac{7}{36}$ (C) $\frac{1}{6}$ (D) $\frac{5}{12}$ (E) $\frac{2}{3}$
14. Uno strano gioco sta affascinando i bambini al Luna Park. In un sacchetto ci sono tre palline di colore diverso. Chi scommette di riuscire ad estrarre in 9 prove successive solo palline di esattamente due diversi colori (l'estrazione di palline tutte dello stesso colore non fa quindi vincere la scommessa) rimettendo ogni volta nel sacchetto la pallina estratta vincerà il quintuplo della scommessa. L'ispettrice Le Blanc, informata del gioco fa subito arrestare i criminali. Determinare la probabilità di vittoria del gioco.
15. Qual è la probabilità di vincere o pareggiare tirando un solo dado a sei facce contro un avversario che ne lancia due sommandone i valori?
16. I tre piatti di Rico, Kowalsky e Soldato contengono ciascuno un pesce. Skipper, bendato, per cinque volte consecutive toglie un pesce da un piatto e lo sposta in un altro. Quale è la probabilità che alla fine degli spostamenti i tre piatti contengano tutti solo un pesce?

4.9.3 Esercizi proposti

Combinatoria

1. Ad una gara a punti su pista partecipano nove concorrenti. Ad ogni traguardo intermedio vengono assegnati 9 punti al primo, 8 al secondo, 7 al terzo e così via fino ad assegnare un punto all'ultimo.
Prima dell'ultimo sprint (in cui il punteggio assegnato vale il doppio) la classifica vede al comando Alberto con 2 punti di vantaggio su Boris e 9 su Claudio. Gli altri concorrenti hanno un distacco in punti tale da non consentire più loro di aggiudicarsi la gara.
Quanti sono i possibili differenti piazzamenti dei tre corridori nell'ultimo sprint che permettono a Claudio di vincere la gara?
2. Ogni partito ha fatto le sue promesse; due partiti qualunque hanno almeno una promessa in comune, due partiti diversi non hanno fatto esattamente le stesse promesse. Sapendo che le promesse totali sono al più 5, qual'è il numero massimo di partiti presenti?
3. In quanti modi è possibile colorare con sei colori un pentagono dodecaedro in modo che ogni faccia confini con cinque facce di colori diversi fra loro e da quello della faccia stessa?
4. Per numerare i biglietti di una lotteria è stata usata 999 volte la cifra 9 (i numeri dei biglietti vanno dal numero 1 in poi). Quanti biglietti sono stati emessi per la lotteria?
5. Siano A_1, A_2, \dots, A_{n+1} insiemi aventi ciascuno n elementi, tali che ogni coppia di insiemi abbia esattamente un elemento in comune e che ogni elemento dell'unione appartenga

ad esattamente 2 insiemi. Per quali valori di n è possibile colorare con 2 colori gli elementi dell'unione in modo che ogni insieme possieda un ugual numero di elementi dei due colori?

6. Si determini il numero di regioni in cui una superficie sferica è suddivisa da n cerchi massimi tale che nessun punto appartenga a tre di essi.
7. Dato un cubo C , quanti sono i triangoli che hanno per vertici tre vertici di C e che non giacciono su nessuna delle facce di C ?
8. In un torneo di pallacanestro ogni squadra affronta esattamente due volte tutti gli altri partecipanti. Il torneo viene vinto da una squadra sola in testa alla classifica con 26 punti, mentre esattamente 2 squadre arrivano ultime con 20 punti. Quante squadre hanno partecipato al torneo? (Ricordiamo che nella pallacanestro si assegnano 2 punti alla vittoria e nessuno alla sconfitta, mentre non è possibile pareggiare)
9. Una regione contiene diciassette città; ognuna di esse è collegata ad esattamente altre 8 con un volo diretto (andata e ritorno). Dimostrare che da ogni città se ne può raggiungere qualsiasi altra.
10. Sia dato un rettangolo $m \times n$ quadratini unitari. Quanti quadratini sono attraversati da una diagonale del rettangolo?
11. Siano dati 8 punti distinti nel piano. Vengano costruiti tutti i possibili segmenti con estremi in tali punti. Si sa che gli assi di almeno 22 di questi segmenti si intersecano in uno stesso punto. Si dimostri che tutti gli assi dei segmenti costruiti si intersecano nel medesimo punto.
12. Una pedina deve muoversi dalla casella A alla casella B spostandosi solo in orizzontale o verticale di una casella alla volta. Quanti sono i percorsi minimi da A a B? Fra questi, quanti tali che la pedina non si muove verso il basso in due mosse consecutive?

A					
					B

13. $A = \{1, 2, \dots, n\}$. Quante sono le coppie $\langle B, C \rangle$ di sottoinsiemi disgiunti di A ? (si considerino coppie NON ordinate) [suggerimento: considerare le coppie per numero totale k di elementi. Quindi $k = |B \cup C| = |B| + |C|$. Per ogni k ci sono $C_{n,k}$ possibili scelte fra gli elementi di $A \dots$]
14. Siano dati 8 punti distinti nel piano. Vengono costruiti tutti i possibili segmenti con estremi in tali punti. Si sa che gli assi di almeno 22 di questi segmenti si intersecano in uno stesso punto. Si dimostri che tutti gli assi dei segmenti costruiti si intersecano nel medesimo punto.
 (A) 12 (B) 24 (C) 32 (D) 56 (E) 112

15. Data una schedina contenente n partite, determinare quante sono le possibili colonne che contengono un numero pari di pareggi.
16. Per aprire una cassaforte, Arsenio Lupin deve girare una manopola: ad ogni scatto, essa permuta, sempre secondo lo stesso schema, 7 meccanismi della serratura. Per aprirla, la configurazione deve essere identica a quella iniziale. Sapendo che la manopola gira sempre nello stesso verso e quando Lupin comincia a scassinarla non sa in quale posizione siano i meccanismi, qual è il massimo numero di tentativi che può fare prima di riuscire ad aprirla?
17. Consideriamo la funzione data da

x	1	2	3	4	5
$f(x)$	4	1	3	5	2

Se $\{u_n\}$ è una successione definita da

$$u_0 = 4, \quad u_{n+1} = f(u_n)$$

quanto vale u_{2010} ?

18. In quante regioni viene diviso un piano da 2010 rette, tali che non ne esistono 2 parallele e non ne esistono 3 che passano per uno stesso punto?
19. Si vogliono riempire le nove caselle di una tabella 3x3 con interi non negativi, in maniera tale da rispettare le seguenti condizioni:
- in almeno una delle caselle viene inserito il numero 3;
 - la somma dei numeri in ciascuna riga è 3;
 - la somma dei numeri in ciascuna colonna è 3.

In quanti modi differenti possiamo riempire la tabella?

(A) 18 (B) 24 (C) 27 (D) 30 (E) 36

20. Il pianeta di Faerun, secoli dopo gli eventi di D & D, è diventato un mondo sviluppato come la Terra di oggi. In particolare, è presente una rete stradale internazionale, che si estende anche su tutti i mari e gli oceani, le cui strade sono numerate da 1 a 30000, un po' come le statali italiane lo sono da 1 a 700. Tuttavia, questa rete presenta delle caratteristiche particolari: ogni strada collega esattamente due città, nessuna strada si incrocia con altre strade, e in qualunque punto del pianeta io mi trovi sarò racchiuso da esattamente 3 strade. Quante sono le città?

Probabilità

21. Una scatola contiene 3 palline bianche e 2 palline nere. Marco estrae una pallina e la rimette nella scatola aggiungendo un'altra pallina dello stesso colore. A questo punto

egli estrae una nuova pallina dalla scatola. Qual'è la probabilità che quest'ultima sia bianca?

22. Qual è il minimo numero di lanci di un dado che devono essere fatti per avere una probabilità superiore al 50% che la somma di tutti i punteggi ottenuti sia maggiore o uguale a 48?
23. Se si butta una moneta di diametro 2 cm su di una scacchiera 8×8 di lato 60 cm qual è la probabilità che la moneta cada interamente in una casella della scacchiera?
24. Giorgio va alla gara di Febbraio, composta da 20 quesiti a risposta multipla. Si supponga che Giorgio provi a dare le risposte basandosi sul caso.
- Qual è la probabilità che li sbagli tutti?
 - Qual è la probabilità che ne faccia giusti esattamente 7?
 - Qual è la probabilità che ne faccia giusti almeno 5?
 - Qual è la probabilità che ne faccia giusti almeno 16?

25. Il tuo liceo è in finale nazionale! Però deve rispondere all'ultima domanda utilizzando solo uno dei componenti della squadra.

Viene deciso che sarà la sorte a scegliere chi di loro avrà questa responsabilità, tirando un dado da 7).

Sapendo che la probabilità che un componente dia la risposta giusta è:

Alberto 50%

Stefano 50%

Giorgio 40%

Riccardo 40%

Marco 30 %

Davide 20%

Edoardo 10%

- Qual è la probabilità che il tuo liceo vinca?
 - Qual è la probabilità che vinca, sapendo che è stato estratto Edoardo?
 - Qual è la probabilità che sia stato estratto Giorgio, sapendo che il tuo liceo non ha vinto?
26. Alessia e Matteo fanno un bellissimo e divertente gioco in una Casetta: a turno ognuno dice una lettera a caso, fino ad ottenere una parola di sei lettere. Qual è la probabilità che essa sia pronunciabile, cioè che sia costituita da un alternarsi di consonanti e vocali qualsiasi?
27. Luca ha in mano dieci pezzetti di carta con le 10 cifre scritte sopra. Li mischia fino ad ottenere una sequenza casuale.
- Qual è la probabilità che il numero da lui ottenuto sia di 10 cifre e:
- divisibile per 2?

- divisibile per 5?
 - divisibile per 3?
 - divisibile per 6?
 - divisibile per 2 o per 3?
28. Si lancia n volte un dado, con le facce contrassegnate da 1 a 6. Qual è la probabilità che la somma dei punteggi usciti sia divisibile per 7.
29. Consideriamo 27 antenne indistinguibili disposte allineate. Di esse 6 sono rotte. Una disposizione è funzionante se non vi compaiono due antenne consecutive rotte.
- Quante sono le disposizioni funzionanti?
 - Qual è la probabilità di avere una disposizione funzionante?
30. In una città molto popolosa, lo 0.1% della popolazione sotto i 50 anni possiede il gene di una grave malattia che si manifesta poi in età avanzata. E' in fase di sviluppo un test per rilevare la presenza di questo gene. Al momento il test sbaglia una volta su 100. Inoltre, ogni anno la probabilità d'errore viene abbassata del 5%. Per risparmiare costose cure mediche, il test sarà ritenuto utile e brevettato se meno del 5% delle persone risultate positive al test (i "presunti malati") è in realtà sano.
- Attualmente, qual è la probabilità che un individuo risultato positivo sia in realtà sano?
 - A quale margine d'errore si vuole arrivare per brevettare il test? Quanti anni mancano perché ciò accada?
31. Alberto vuole organizzare per questa sera una partita a poker. Egli sa che Bruno e Barbara si recano insieme in palestra una sera su tre, e che Carla, Corrado, Dario e Davide sono impegnati una sera su due (ma non necessariamente negli stessi giorni). Inoltre sa che Dario non vuole giocare a poker con Davide. poiché per giocare servono almeno 4 persone (compreso Alberto), qual è la probabilità che stasera si giochi?
32. Provate a studiare, in via teorica, il seguente problema:
Ci sono 6 eventi tali che:

La probabilità che avvenga l'evento k è p_k ;

$$\sum_{k=1}^6 p_k = 1$$

Esistono due eventi che hanno diverse probabilità di accadere.

Il gioco finisce quando l'evento si verifica 10 volte.

- Qual è la probabilità che il gioco finisca dopo 10 giocate?
- Qual è la probabilità che il gioco finisca dopo 15 giocate?
- Qual è la probabilità che il gioco finisca perché accade 10 volte l'evento k ?

33. Qual è la probabilità che, presi a caso tre vertici distinti di un esagono regolare, essi siano i vertici di un triangolo equilatero?
(A) $\frac{1}{4}$ (B) $\frac{1}{8}$ (C) $\frac{1}{9}$ (D) $\frac{1}{10}$ (E) $\frac{1}{20}$
34. Un gioco consiste nel lancio ripetuto di un dado; i punteggi ottenuti ad ogni lancio vengono sommati al totale precedente e un giocatore vince tanti gettoni qual è il suo punteggio, ma non vince nulla se il suo punteggio supera 10. A partire da quale punteggio conviene scegliere di fermarsi e ritirare il premio?
35. Nella classe di Pippi Calzelunghe nessuno sa il compleanno degli altri. Tuttavia c'è una quantità di persone tale per cui la probabilità che due compagni festeggino il compleanno lo stesso giorno è superiore al 50%. Se però Pippi ne accoppiasse anche solo uno la probabilità scenderebbe al di sotto di tale cifra. Quanti sono i compagni di classe di Pippi?
36. Ad una cena partecipano 20 uomini e 40 donne; due di queste sono gemelle. Decidono di sedersi in modo tale che non ci siano mai due uomini seduti a fianco. Qual è la probabilità che le due gemelle si trovino sedute a fianco?
37. Un componente di un macchinario è libero di spostarsi su di una struttura a forma di griglia quadrata di dimensioni sufficientemente grandi con quadretti di lato 1 passo. A causa di un virus informatico che ha intaccato il suo sistema di controllo, ad un certo punto il componente, che si trova in posizione (2, 2), inizia a muoversi, decidendo ad ogni vertice della griglia di prendere casualmente una direzione, ognuna con la stessa probabilità delle altre. Qual è la probabilità che, dopo 13 passi, si trovi al punto (-4, -4)?
38. Tirando 6 dadi a 6 facce non truccati, qual è la probabilità, in percentuale, che la somma dei valori ottenuti sia dispari?

La *geometria* è l'argomento dei problemi olimpici che meglio si spiega da sè. In pratica quasi tutti i problemi che presentino una figura rientrano in questa categoria, che viene poi divisa in piana e solida, a seconda che le figure siano piane o meno.

Un esagono equiangolo ha quattro lati consecutivi lunghi, nell'ordine, 5, 3, 6 e 7. Determinare le lunghezze degli altri due lati.

5.1 Teoremi

5.1.1 Angolo alla circonferenza

In ogni circonferenza, l'angolo al centro è il doppio di ogni angolo alla circonferenza che insista sul medesimo arco (o sulla medesima corda).

Corollario: Tutti gli angoli alla circonferenza che insistono su archi (o corde) uguali sono uguali. Banale è il fatto che angoli che insistano su una semicirconferenza siano retti. In altre parole, ogni triangolo rettangolo può essere inscritto in una semicirconferenza che abbia come diametro l'ipotenusa stessa.

5.1.2 Angolo esterno

In qualsiasi triangolo, ogni angolo esterno è la somma dei due angoli interni non adiacenti.

5.1.3 Bisettrice

La bisettrice interna di un triangolo divide il lato opposto in parti proporzionali ai due lati che la comprendono.

5.1.4 Due corde

Condotte da un punto M interno ad una circonferenza due corde AB e CD , esse si dividono formando quattro segmenti tali che $AM : MD = CM : MB$.

5.1.5 Euclide 1

In un triangolo rettangolo il quadrato costruito su un cateto è equivalente al rettangolo che ha per lati l'ipotenusa e la proiezione del cateto sull'ipotenusa.

5.1.6 Euclide 2

In un triangolo rettangolo il quadrato costruito sull'altezza relativa all'ipotenusa è equivalente al rettangolo che ha per lati le proiezioni dei cateti sull'ipotenusa.

5.1.7 Secanti

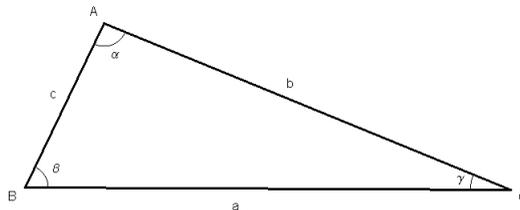
Condotte da un punto P esterno ad una circonferenza due secanti che incontrano la circonferenza rispettivamente in A, B e C, D , si ha che $PD : PB = PA : PC$.

5.1.8 Talete

Due trasversali a e b che incontrano tre rette parallele r_1, r_2, r_3 rispettivamente in A_1, A_2, A_3 e B_1, B_2, B_3 determinano quattro segmenti tali che:

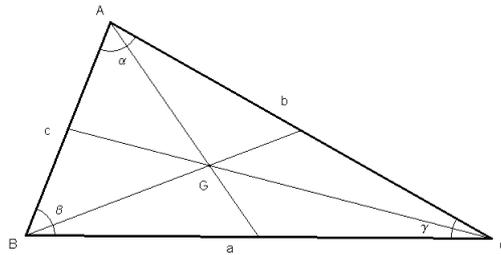
$$\frac{A_1A_2}{B_1B_2} = \frac{A_2A_3}{B_2B_3}$$

5.2 Punti notevoli



5.2.1 Baricentro

Il *baricentro* è il punto in cui concorrono le mediane di un triangolo. Divide ogni mediana in due parti, di cui quella maggiore ha un estremo nel vertice è il doppio dell'altra. Il baricentro è il punto del piano per il quale la somma dei quadrati delle distanze dai vertici è minima.



5.2.2 Circoentro

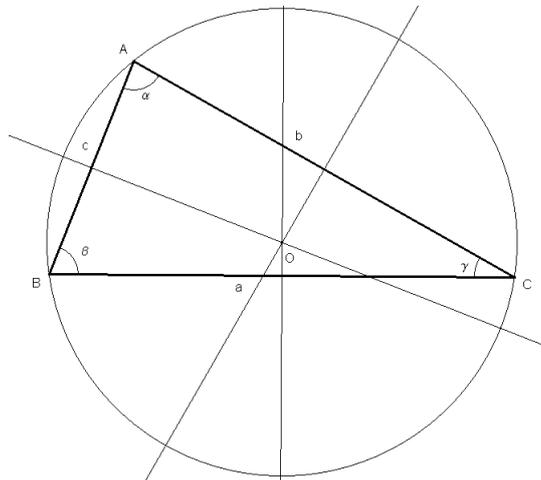
Il *circoentro* è il centro O del cerchio circoscritto al triangolo; ed è quindi il punto d'incontro degli assi dei lati. Se S è l'area del triangolo e a, b, c le misure dei lati, si ha:

$$S = \frac{abc}{4R}$$

dove R è il raggio della circonferenza circoscritta; inoltre si ha:

$$r \cdot R = \frac{abc}{4p}$$

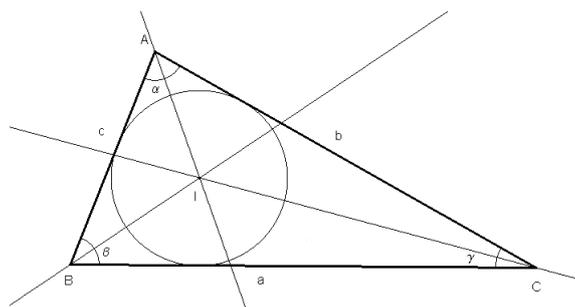
dove r è il raggio della circonferenza inscritta e p il semiperimetro del triangolo.



5.2.3 Incentro

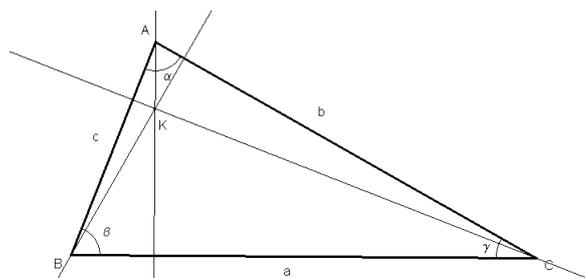
L'*incentro* è il centro del cerchio inscritto al triangolo. Esso è il punto di incontro delle bisettrici interne del triangolo. Se r è il raggio della circonferenza inscritta e p il semiperimetro del triangolo, la sua area S è data da :

$$S = p \cdot r$$



5.2.4 Ortocentro

L'*ortocentro* è il punto di incontro delle tre altezze. I tre vertici del triangolo e l'ortocentro formano un sistema ortocentrico, nel senso che ciascuno di essi è l'ortocentro del triangolo formato dagli altri tre. Il punto simmetrico dell'ortocentro di un triangolo rispetto al lato giace sul cerchio circoscritto al triangolo.



5.3 Criteri

5.3.1 Criteri di congruenza

Due triangoli sono congruenti se vale uno qualunque dei seguenti fatti equivalenti:

- hanno due lati uguali e l'angolo compreso uguale
- hanno due angoli uguali e il lato compreso uguale.
- hanno i tre lati uguali
- hanno un lato uguale, l'angolo adiacente e l'angolo opposto uguali.
- hanno due lati uguali, l'angolo opposto ad uno di essi uguale e gli angoli opposti all'altro lato sono della stessa specie.

5.3.2 Criteri di similitudine

Due triangoli sono simili se vale uno qualunque dei seguenti fatti equivalenti:

- hanno i tre angoli uguali
- hanno i tre lati in proporzione
- hanno due lati in proporzione e l'angolo compreso uguale.
- hanno due lati in proporzione, l'angolo opposto ad uno di essi uguale e gli angoli opposti all'altro lato sono della stessa specie.

5.3.3 Criteri di circoscrivibilità e inscrivibilità

Ogni triangolo è sia circoscrivibile che inscrivibile in un cerchio.

Un quadrilatero convesso è circoscrivibile ad un cerchio se e solo se la somma di due lati non consecutivi è uguale alla somma degli altri due lati.

Un quadrilatero convesso è inscrivibile ad un cerchio se e solo se gli angoli opposti sono supplementari.

5.4 Formule per il calcolo geometrico

5.4.1 Diseguaglianza triangolare

Chiamando a e b i due lati di un triangolo e c il terzo lato, ovvero la loro somma vettoriale $a + b$, si ha che

$$\left| \|a\| - \|b\| \right| \leq \|a + b\| \leq \|a\| + \|b\|$$

dove il simbolo $\|\cdot\|$ rappresenta la lunghezza di un segmento. Questa disuguaglianza può essere riformulata come “in un triangolo ogni lato è minore della somma degli altri due e maggiore della loro differenza”, che costituisce un criterio per la costruttibilità o meno del triangolo stesso.

5.4.2 Calcolo dell'area

Triangolo: $A = \frac{1}{2} \cdot b \cdot h$

Parallelogramma: $A = b \cdot h$

Trapezio: $A = \frac{1}{2} \cdot h \cdot (B + b)$

Rombo: $A = \frac{1}{2} \cdot d_1 \cdot d_2$ (si noti che il rombo è anche un parallelogramma)

Poligono regolare di n lati: $A = \frac{1}{2} \cdot n \cdot l \cdot a$ dove a sta per apotema

Cerchio: $A = \pi r^2$

Settore circolare: $A = \frac{\alpha}{360} \cdot \pi r^2$ dove α è la misura dell'angolo espressa in gradi

5.4.3 Calcolo del volume

Prisma: $V = A_b \cdot h$

Piramide retta: $V = \frac{1}{3} \cdot A_b \cdot h$

Cilindro: $V = \pi r^2 h$

Cono: $V = \frac{1}{3} \pi r^2 h$

Sfera: $V = \frac{4}{3}\pi r^3$

5.4.4 Raggi

Raggio della circonferenza circoscritta: $R = \frac{abc}{4A}$

Raggio della circonferenza inscritta: $r = \frac{A}{p}$

5.4.5 Formula di Erone

Detti a, b, c i lati di un triangolo qualsiasi e p il semiperimetro di tale triangolo, l'area A del triangolo vale:

$$A = \sqrt{p(p-a)(p-b)(p-c)}$$

5.4.6 Formula di Eulero

In ogni poliedro convesso se F è il numero delle facce, S il numero degli spigoli e V il numero dei vertici si ha :

$$F - S + V = 2$$

Soluzione problema di inizio capitolo.

Indichiamo con $AB = 5$, $BC = 3$, $CD = 6$, $DE = 7$, $EF = x$ e $FA = y$. Poiché l'esagono risulta equiangolo, per costruire i primi 4 lati consecutivi basta tracciare 4 segmenti contigui delle rispettive lunghezze e inclinati a due a due di 120 gradi. La soluzione più veloce consiste nel prolungare i segmenti BC , DE e FA fino ai loro punti di incontro, A' , B' e C' . Il triangolo $A'B'C'$ risulta equilatero (perché?), con $A'B' = 5 + 3 + 6 = 14$, $B'C' = 6 + 7 + x = 13 + x$ e $C'A' = x + y + 5$. Ma poiché $A'B'C'$ è equilatero, deve essere $13 + x = 5 + x + y = 14$, da cui $x = 1$ e $y = 8$.

5.5 Approfondimenti

Di geometria, approfondiamo solamente alcune formule di calcolo in vista della preparazione alle gare nazionali.

5.5.1 Calcolo sintetico

Notazioni standard. Per i triangoli sono solitamente usate queste notazioni:

- A, B, C sono i vertici.
- a, b, c sono le lunghezze dei lati opposti ad A, B, C rispettivamente; $p = (a + b + c)/2$ è il semiperimetro, ed S è l'area.

- α, β, γ sono le ampiezze degli angoli opposti a a, b, c .
- K, G, O, I sono rispettivamente ortocentro, baricentro, circocentro e incentro del triangolo.
- r ed R sono rispettivamente i raggi della circonferenza inscritta e circoscritta.

Area di un triangolo. L'area di un triangolo può essere calcolata come:

$$S = \sqrt{p(p-a)(p-b)(p-c)} = \frac{1}{4} \sqrt{(a^2 + b^2 + c^2)^2 - 2(a^4 + b^4 + c^4)}$$

Area di un quadrilatero inscritto. Un quadrilatero inscritto ha area:

$$S = \sqrt{(p-a)(p-b)(p-c)(p-d)}$$

Retta di Eulero. I tre punti K, G, O sono allineati, e vale la relazione $KG = 2GO$. Secondo la notazione prima specificata, vale anche la cosiddetta Formula di Eulero $OI^2 = R^2 - 2rR$.

Mediane. Dette m_a, m_b, m_c le mediane uscenti da A, B, C , si ha:

$$m_a = \frac{1}{2} \sqrt{2(b^2 + c^2) - a^2}$$

$$m_b = \frac{1}{2} \sqrt{2(a^2 + c^2) - b^2}$$

$$m_c = \frac{1}{2} \sqrt{2(b^2 + a^2) - c^2}$$

Bisettrici. Dette d_a, d_b, d_c le bisettrici uscenti da A, B, C , si ha:

$$d_a = \frac{2}{b+c} \sqrt{bc p(p-a)}$$

$$d_b = \frac{2}{a+c} \sqrt{ac p(p-b)}$$

$$d_c = \frac{2}{b+a} \sqrt{ba p(p-c)}$$

Altezze. Dette h_a, h_b, h_c le altezze uscenti da A, B, C , si ha:

$$h_a = \frac{2S}{a} = \frac{2}{a} \sqrt{p(p-a)(p-b)(p-c)}$$

$$h_b = \frac{2S}{b} = \frac{2}{b} \sqrt{p(p-a)(p-b)(p-c)}$$

$$h_c = \frac{2S}{c} = \frac{2}{c} \sqrt{p(p-a)(p-b)(p-c)}$$

Angoli. In un triangolo, c'è un rapido calcolo per verificare la specie di un angolo:

- se $a^2 < b^2 + c^2$ allora α è acuto
- se $a^2 = b^2 + c^2$ allora α è retto
- se $a^2 > b^2 + c^2$ allora α è ottuso

Per i raggi delle circonferenze ex-inscritte (tangenti ai lati prolungati del triangolo) abbiamo che:

$$r_a = \frac{S}{p-a}, \quad r_b = \frac{S}{p-b}, \quad r_c = \frac{S}{p-c}$$

Uguaglianza di Tolomeo. Siano $ABCD$ quattro punti presi in ordine su una circonferenza (cioè $ABCD$ è un quadrilatero ciclico), allora:

$$AB \cdot CD + AD \cdot BC = AC \cdot BC$$

5.5.2 Calcolo trigonometrico

Relazione fondamentale. Per ogni angolo θ si ha $\cos^2 \theta + \sin^2 \theta = 1$

Formule di addizione e sottrazione. Valgono le seguenti relazioni:

$$\sin(\alpha + \beta) = \sin \alpha \cos \beta + \cos \alpha \sin \beta \quad \sin(\alpha - \beta) = \sin \alpha \cos \beta - \cos \alpha \sin \beta$$

$$\cos(\alpha + \beta) = \cos \alpha \cos \beta - \sin \alpha \sin \beta \quad \cos(\alpha - \beta) = \cos \alpha \cos \beta + \sin \alpha \sin \beta$$

$$\sin 2\alpha = 2 \sin \alpha \cos \alpha \quad \cos 2\alpha = \cos^2 \alpha - \sin^2 \alpha = 2 \cos^2 \alpha - 1 = 1 - 2 \sin^2 \alpha$$

Formule di Werner e Prostaferesi. Valgono le seguenti relazioni:

$$2 \sin \alpha \sin \beta = \cos(\alpha - \beta) - \cos(\alpha + \beta)$$

$$2 \sin \alpha \cos \beta = \sin(\alpha + \beta) + \sin(\alpha - \beta)$$

$$2 \cos \alpha \cos \beta = \cos(\alpha + \beta) + \cos(\alpha - \beta)$$

$$\sin \alpha + \sin \beta = \sin \frac{\alpha + \beta}{2} \cos \frac{\alpha - \beta}{2}, \quad \sin \alpha - \sin \beta = 2 \cos \frac{\alpha + \beta}{2} \sin \frac{\alpha - \beta}{2}$$

$$\cos \alpha + \cos \beta = 2 \cos \frac{\alpha + \beta}{2} \cos \frac{\alpha - \beta}{2} \quad \cos \alpha - \cos \beta = 2 \sin \frac{\alpha + \beta}{2} \sin \frac{\alpha - \beta}{2}$$

Parametrizzazione. Posto $t = \tan \alpha/2$, si ha:

$$\sin \alpha = \frac{2t}{1+t^2} \quad \cos \alpha = \frac{1-t^2}{1+t^2}$$

Area di un triangolo. In un triangolo, vale la relazione:

$$S = \frac{1}{2} ab \sin \gamma = \frac{1}{2} cb \sin \alpha = \frac{1}{2} ca \sin \beta$$

Teorema di Carnot. In un triangolo $c^2 = a^2 + b^2 - 2ab \cos \gamma$.

Teorema dei seni. Valgono le seguenti relazioni:

$$2R = \frac{a}{\sin \alpha} = \frac{b}{\sin \beta} = \frac{c}{\sin \gamma}$$

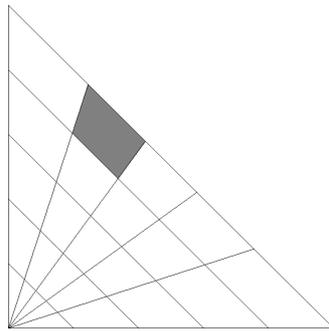
$$r = (p-a) \tan \frac{\alpha}{2} = (p-b) \tan \frac{\beta}{2} = (p-c) \tan \frac{\gamma}{2}$$

5.6 Esercizi

5.6.1 Esercizi svolti

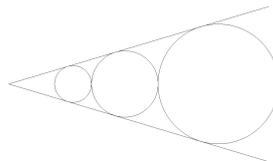
1. Nel triangolo rettangolo isoscele disegnato in figura 5.1, ogni lato è stato diviso in cinque parti uguali. Determinare l'area della regione evidenziata in grigio sapendo che ciascun cateto è lungo 50 cm.

Figura 5.1:



2. Tre circonferenze C_R , C_x , C_r (figura 5.2), di raggio rispettivamente uguale a R , x , r , hanno i centri allineati. Si sa che C_R e C_r sono tangenti esternamente a C_x e che le tre circonferenze hanno due tangenti esterne in comune. Noti r , R , quanto vale x ?

Figura 5.2:

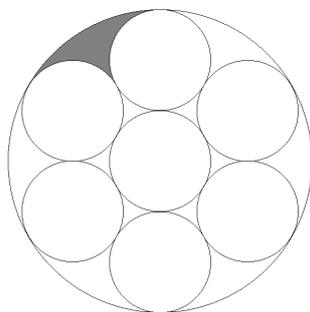


3. Nella figura 5.3 il raggio dei cerchi piccoli è 1. Quanto vale l'area della figura tratteggiata?
4. Una sfera di raggio $r = 15$ cm è appoggiata su due binari distanti tra loro 24 cm. Se la sfera effettua una rotazione completa, di quanto avanza sui binari?
5. In un cubo di lato 12, P e Q sono i centri di due facce che hanno in comune lo spigolo AB . Qual è il volume del tetraedro che ha per vertici i punti A ; B ; P e Q ?

5.6.2 Esercizi proposti

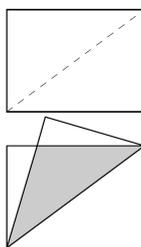
1. Dimostrare che un quadrilatero convesso è circoscrittibile ad un cerchio se e solo se la somma di due lati non consecutivi è uguale alla somma degli altri due lati.

Figura 5.3:



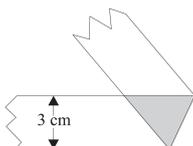
2. Dimostrare che un quadrilatero convesso è inscrittibile ad un cerchio se e solo se gli angoli opposti sono supplementari.
3. Dato un foglio rettangolare di lati a e b , con $a > b$, determinare l'area del triangolo che risulta dalla sovrapposizione dei due lembi che si ottengono piegando il foglio lungo una diagonale (il triangolo ombreggiato nella figura 5.4).

Figura 5.4: testo



4. Una striscia di carta con bordi paralleli distanti 3 cm viene piegata in modo che una parte di essa risulti parzialmente sovrapposta alla parte rimanente (vedi figura 5.5). Qual è l'area minima della zona ombreggiata?

Figura 5.5: testo



5. Sia P_1 un esagono regolare. Sia P_2 un esagono ottenuto congiungendo i punti medi dei lati consecutivi di P_1 . Allo stesso modo si proceda a partire da P_2 ottenendo un nuovo esagono P_3 . Quanto vale il rapporto tra l'area di P_3 e quella di P_1 ?

6. Il diametro BC di una circonferenza è anche la base di un triangolo isoscele ABC i cui altri lati tagliano la circonferenza nei punti D ed E . Detto O il centro della circonferenza, e sapendo che l'angolo DOE misura 100 gradi, dire quanto misura l'angolo BAC .
7. Un contenitore ha la forma di un cono circolare retto avente altezza uguale a 1 metro e diametro uguale a 2 metri. Il cono è posto verticalmente con la punta verso il basso e contiene un fluido che raggiunge l'altezza di x metri. Sul contenitore viene fatto un segno in corrispondenza dell'altezza raggiunta dal fluido. Sapendo che, rovesciando il cono con la punta verso l'alto, l'altezza del fluido arriva esattamente al segno fatto in precedenza, calcolare il valore di x .
8. Si consideri un quadrato $ABCD$ di lato 16 metri. Su due lati consecutivi AB e BC si costruiscano, esternamente rispetto al quadrato, i due triangoli equilateri ABE e BCF . Quanto vale l'area del triangolo BEF in metri quadrati?
9. In un quadrilatero convesso $ABCD$ i lati AB , BC , CD sono uguali. Inoltre $AC = BD = AD$. Quanto misura l'angolo in D ?
10. Dimostrare che un pentagono iscritto in una circonferenza e tale che ogni sua diagonale sia parallela ad un lato, è necessariamente regolare.
11. Sia $ABCD$ un trapezio con base maggiore AB tale che le diagonali AC e BD siano perpendicolari. Sia O il centro della circonferenza circoscritta al triangolo ABC e sia E il punto di intersezione tra la retta OB e la retta CD . Dimostrare che

$$BC^2 = CD \cdot CE$$

12. Sia P un punto interno ad un triangolo equilatero ABC tale che $AP = 3$, $BP = 4$, $CP = 5$. Determinare la lunghezza del lato di ABC .
13. Siano α un cerchio, A un punto interno ad esso e PQ una corda passante per A che non sia un diametro. Chiamiamo p e q le rette tangenti alla circonferenza rispettivamente in P e Q . Sapendo che la retta l passante per A e perpendicolare ad OA interseca p e q nei punti K e L , dimostrare che $\overline{AK} = \overline{AL}$.
14. L'angolo in A di un triangolo ABC misura 30 gradi e il lato AB ha lunghezza 10. La lunghezza del lato BC è uno degli elementi dell'insieme $\{3, 5, 7, 9, 11\}$. Quanti triangoli differenti soddisfano queste condizioni?
15. Un parallelepipedo retto ha spigoli di lunghezza a , b , c con $a < b < c$. Di quale spigolo si deve aumentare la lunghezza di una quantit q affinché si abbia il massimo incremento di volume?
16. Un prisma retto di altezza l e avente per base un esagono regolare di lato l viene tagliato con un piano passante per due spigoli paralleli appartenenti ciascuno ad una delle due basi, ma non appartenenti alla stessa faccia laterale. Qual è l'area della sezione risultante?
17. In un cubo di lato 12, P e Q sono i centri di due facce che hanno in comune lo spigolo AB . Qual è il volume del tetraedro che ha per vertici i punti A , B , P , Q ?

-
18. Sia $ABCD$ un tetraedro generico di cui si conosce la lunghezza a dello spigolo AB e l'area S della proiezione del tetraedro su un piano perpendicolare alla retta per A e B . Determinare il volume del tetraedro.
19. Il punto M varia su una circonferenza γ che passa per due punti fissati A e B . Chiamiamo K il punto medio del segmento MB e r la retta passante per il punto K perpendicolare a MA .
- a) Provare che, fissata la circonferenza γ , tutte le possibili rette r passano per uno stesso punto P .
- b) Trovare l'insieme di tutti i possibili punti P al variare della circonferenza γ tra tutte quelle che passano per A e B .
20. Determinare la lunghezza minima di un laccio chiuso attraverso il quale si può far passare un tetraedro regolare di lato l .

Sono qui riportate le soluzioni per gli esercizi svolti presenti nei capitoli.

6.1 Logica e Matematizzazione

1. Dividiamo il quadrato in 4 quadrati di lato 5 cm . Per il principio dei cassetti, avendo 5 punti e 4 quadrati in almeno un quadrato ci saranno 2 punti. Questi 2 punti hanno ovviamente distanza inferiore alla diagonale del quadrato e quindi distanza inferiore a $5\sqrt{2}$.
2. Si può facilmente notare che premendo il pulsante di tutte le lampadine su una riga e di tutte quelle su una colonna, tutte le lampadine del pannello cambiano di stato un numero pari di volte tranne la lampadina che sta all'incrocio della riga e della colonna. In definitiva queste mosse consentono di accendere una lampadina lasciando le altre inalterate. Si può quindi raggiungere la configurazione in cui sono tutte accese a partire da qualsiasi configurazione iniziale.
3. La risposta è **(B)**. Per separare il quadretto cattivo occorrono due tagli (i due lati per cui è attaccato alla tavoletta), quindi chi fa il primo dei due perde, perché l'altro può così isolare il quadretto cattivo. Se Roberto sceglie la mossa (C) o la mossa (D) fa questo taglio, se sceglie la mossa (B) invece costringe Marco a fare uno di questi due tagli, e può così fare il secondo vincendo.
4. Mentre a compie un giro b compie $\frac{14}{15}$ di giro, c ne compie $\frac{14}{16}$ ($=\frac{7}{8}$) e d ne compie $\frac{14}{18}$ ($=\frac{7}{9}$). Occorre dunque trovare il più piccolo intero n che moltiplicato per le frazioni precedenti dia per risultato un numero intero. Questo è ovviamente il minimo comune multiplo dei denominatori 15,8,9 che è 360.

6.2 Teoria dei Numeri

1. La risposta è **(B)**.
La successione degli scalini toccati dal canguro è $3-1+5-3+7-5+\dots$. Tale successione può essere riscritta come $(3-1)+(5-3)+(7-5)+\dots$, dalla quale è immediato verificare che il canguro tocca tutti gli scalini pari; inoltre può essere riscritta anche come $3+(-1+5)+(-3+7)+\dots$, dalla quale appare chiaro che il canguro tocca tutti gli scalini della forma

$4k + 3$. Dunque il canguro non cadrà solo se lo scalino pericolante è della forma $4k + 1$, nel nostro caso 2001.

2. La risposta è (E).

Osserviamo che $\sum_0^k (2i + 1) = \sum_0^k (2i) + \sum_0^k 1 = 2 \sum_0^k i + k + 1 = k(k + 1) + k + 1 = (k + 1)^2$. Si prova facilmente che tutti i risultati sono quadrati perfetti tranne 4525.

3. La risposta è (D).

Quando si considerano le potenze di un intero x modulo un qualche n (in questo caso $n = 10$), come abbiamo visto importa solo il valore $x \bmod n$ (in questo caso $x \bmod 10$ cioè la cifra delle unità). Se si moltiplica un numero che ha 7 come cifra delle unità ripetutamente per se stesso, si prova che si ottengono numeri che hanno come cifra delle unità la prima volta 9, la seconda 3, la terza 1 e la quarta nuovamente 7. Dunque la cifra delle unità delle potenze di 2137 sono 7, 9, 3, 1, 7, 9, 3, 1, 7, ... e si ripetono ogni 4. Siccome $753 = 1 + 4 \cdot 188$, la cifra delle unità di 2137^{753} è la stessa di 2137, cioè 7. Notiamo che l'elevamento a potenza è una classica operazione ripetuta.

4. La risposta è (E).

Possiamo scrivere $n = q1995 + 29$ e quindi l'ultima cifra di n può essere solo 9 (se q è pari) o 4 (se q è dispari). Ma poiché n diviso per 1996 dà resto dispari, n è dispari, e la sua cifra delle unità è 9.

5. Si ha che $n^2 - 14n + 24 = (n - 2)(n - 12)$ è primo solo se uno dei due fattori è 1 o -1: nel primo caso $n = 13$, che effettivamente dà come risultato 11, e $n = 3$ che dà come risultato -9, che non è primo; nel secondo caso $n = 1$ che dà come risultato 11 che è primo, e $n = 11$ che dà come risultato -9, che non è primo. Le soluzioni sono quindi $n = 1, 13$.

6. L'equazione è verificata quando:

- la base è 1, ovvero $x^2 - x - 1 = 1$, che dà come soluzione 2 e -1.
- la base è -1 e l'esponente è pari, ovvero $x^2 - x - 1 = -1$, che ha come soluzioni 0 e 1, nel primo caso l'esponente è pari, nel secondo dispari, quindi 1 è da scartare.
- l'esponente è 0, ovvero $x = -2$, valore per cui la base è diversa da 0.

Ricapitolando, le soluzioni sono 2, -1, 0, -2.

7. Effettuiamo la decomposizione $a^2 - 4b^2 = (a + 2b)(a - 2b) = 45 = 5 \cdot 3 \cdot 3$. Ricordandoci che $a + 2b$ deve essere maggiore di $a - 2b$, possiamo impostare i sistemi:

- $(a + 2b = 9, a - 2b = 5)$, con soluzione (7, 1)
- $(a + 2b = 15, a - 2b = 3)$, con soluzione (9, 3)
- $(a + 2b = 45, a - 2b = 1)$ con soluzione (23, 11).

8. La risposta è (C).

Si osserva che tutte le possibili risposte sono prodotti: se uno dei fattori è divisibile per 3, lo sarà ovviamente anche il prodotto. Si osserva anche che nel prodotto $n(n+2)(n+4)$ i tre fattori sono tutti incongruenti modulo 3: segue che uno di questi è sempre divisibile per 3.

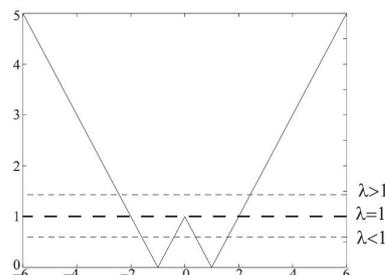
9. La risposta è (E).

Siccome $21ab^2$ è un quadrato, deve esserlo anche $21a$ (il prodotto di quadrati è un quadrato). Se un numero x divide un quadrato perfetto y^2 , allora anche x^2 deve dividere y^2 (è come dire che gli esponenti dei numeri primi che compaiono nella fattorizzazione di un quadrato y^2 sono tutti pari). Quindi 21 divide a , e per ottenere il minimo valore possibile di $a + b$ si pone $a = 21$, che rende $21ab^2 = (21b)^2$ un quadrato. Per quanto riguarda $15ab$, si sostituisce $a = 21$ ottenendo $15 \cdot 21 \cdot b = 3^2 \cdot 5 \cdot 7 \cdot b$. Il minimo valore di b che lo rende un quadrato è quindi $5 \cdot 7 = 35$. Si ricava $a + b = 21 + 35 = 56$.

10. Se si chiama $r \geq 1$ la ragione della progressione, i quattro numeri sono $a, b = a + r, c = a + 2r, d = a + 3r$ e devono essere compresi tra 1 e 100. Segue che $a \geq 1$ e $a + 3r \leq 100$, e quindi $3r \leq 100 - a \leq 99$, ovvero $1 \leq r \leq 33$. Invece, scelto un valore di r , $1 \leq a \leq 100 - 3r$ cioè a può assumere $100 - 3r$ valori diversi per ogni r . Si può ottenere adesso il numero cercato di progressioni aritmetiche: $100 - 3 \cdot 1 + 100 - 3 \cdot 2 + 100 - 3 \cdot 3 + 100 - 3 \cdot 4 + \dots + 100 - 3 \cdot 33 = 33 \cdot 100 - 3(1 + 2 + 3 + 4 + \dots + 33) = 3300 - 3 \cdot \frac{33 \cdot 34}{2} = 3300 - 1683 = 1617$.

6.3 Algebra

- Osserviamo che $P(1) = \sum_{i=0}^n a_i$, cioè la somma algebrica cercata. Sostituendo il valore 1 nel polinomio si ha $(1 + 4 - 3)^{2001} - (1 + 4 + 3)^{667} + 1 + 4 = 2^{2001} - 2^{3 \cdot 667} + 5 = 5$, che è la soluzione.
- Abbiamo che dividendo $P(x)$ per x si ha come resto a_0 . Dividendo tutte le alternative proposte per il numero in cui è calcolato $P(x)$ si ha $92 \equiv 2 \pmod{3}$, contrariamente all'ipotesi che tutti i coefficienti siano 0 o +1.
- Abbiamo che la somma delle radici è $-a_2$, cioè l'opposto del coefficiente di x^2 , da cui $n + 1 = 0$; ricordandoci che il termine noto è l'opposto del prodotto delle tre radici si ha $1 = -1 \cdot m \cdot 1$, da cui $m = -1$.
- Ci sono soltanto le radici 0 e 3. Infatti, posto $y = 2^x$, si ottiene $9 - y = 8/y$, ossia $y^2 - 9y + 8 = 0$, da cui $y = 1$ o $y = 8$.
- Sia x il numero degli uomini e y il numero delle donne. La media aritmetica è $\frac{35x + 25y}{x + y} = 31$, da cui $4x = 6y$ e $\frac{x}{y} = \frac{3}{2}$.
- Disegnando il grafico, studiamo il sistema facendo variare ad altezza λ una retta parallela all'asse x : si vede che non si hanno soluzioni per λ negativi, due sole soluzioni per $\lambda = 0$, quattro per $0 < \lambda < 1$, tre per $\lambda = 1$, e due oltre.



7. Poiché $(8x^3 + y^3) = (2x + y)(4x^2 - 2xy + y^2)$, si ottiene, sostituendo $y = 1 - 2x$, un'equazione di secondo grado in x data da $4x^2 - 2x(1 - 2x) + (1 - 2x)^2 = k$. Questa equazione deve avere un'unica soluzione reale e annullando il discriminante si ottiene $k = \frac{1}{4}$, dunque esiste un solo valore di k che soddisfa le condizioni richieste.
8. L'insieme dei numeri naturali che in base b si scrivono con k cifre è composto dai numeri compresi tra b^{k-1} e $b^k - 1$, estremi inclusi. Infatti b^{k-1} si scrive con una cifra 1 e $k - 1$ cifre 0, ed è pertanto il primo ad essere costituito da k cifre, mentre b^k si scrive con una cifra 1 e k cifre 0, essendo perciò il più piccolo composto da $k + 1$ cifre, dunque il più grande composto da k cifre è il suo predecessore. In questo caso, con $(b, k) = (10, 3)$ si ottiene l'insieme dei numeri compresi tra 100 e 999, mentre con $(b, k) = (2, 7)$ si ottiene quello dei numeri compresi tra 64 e 127. Facendo l'intersezione si ricava l'insieme degli interi compresi tra 100 e 127, che sono $127 - 100 + 1 = 28$.
9. La risposta è (C). Infatti, se fosse $P(2002) = 2002$, allora $P(X)$ coinciderebbe con la funzione identica $I(X) = X$, che è anche un polinomio, in tre punti. Ora, la funzione $Q(X) = P(X) - I(X)$, che è a sua volta un polinomio, si annullerebbe in questi tre punti, ovvero l'equazione $Q(X) = 0$ ammetterebbe almeno quelle tre soluzioni, e dunque $Q(X)$ sarebbe divisibile per $A(X) = (X - 2000)(X - 2001)(X - 2002)$, che è un polinomio di terzo grado. Ma, essendo $P(X)$ e $I(X)$ rispettivamente polinomi di grado 2 e 1, la loro differenza è un polinomio di grado al più 2, e non può essere divisibile per un polinomio di grado 3, a meno che sia il polinomio nullo, che è pertanto l'unica situazione ammissibile. Ne segue che $Q(X) \equiv 0$, ovvero $P(X) \equiv I(X)$, e pertanto $(a, b, c) = (0, 1, 0)$, che non va bene poiché avevamo supposto $a \neq 0$. (anche perché, se $a = 0$, il polinomio non può nemmeno dirsi di secondo grado).
10. Possiamo scrivere:

$$x^2 - 8xy + 19y^2 - 6y + 14 = x^2 - 8xy + 16y^2 + 3y^2 - 6y + 3 + 11 = (x - 4y)^2 + 3(y - 1)^2 + 11$$

che vale almeno 11 in quanto i quadrati non sono mai negativi. Il valore 11 viene effettivamente raggiunto in quanto è possibile annullare contemporaneamente i quadrati (per $(x, y) = (4, 1)$) ed è pertanto il minimo.

6.4 Combinatoria

1. Per ognuno dei $3!$ modi in cui possono disporsi i ragazzi, esistono $3!$ disposizioni delle ragazze; in totale si hanno quindi $3! \cdot 3 = 36$
2. Senza utilizzare la cifra 2 posso costruire 5 numeri; utilizzando la cifra 2 posso costruire: un numero con una cifra (2), due numeri con due cifre (mettendo la cifra 2 al primo o al secondo posto), e così via, per un totale di $5 + 1 + 2 + 3 + 4 + 5 + 6 = 26$ numeri.
3. Tutti i possibili triangoli che hanno come vertici tre vertici di C sono $\binom{8}{3} = 56$. Su ognuna delle 6 facce giacciono 4 triangoli (equivale a scegliere quale vertice non utilizzare per il triangolo), pertanto i triangoli cercati sono $56 - 6 \cdot 4 = 32$.

e Lorenzo devono aver vinto 4 volte ciascuno. La probabilità cercata è quindi $(84) \cdot (4/7)^4 \cdot (3/7)^4$.

- Perché Francesco vinca alla settima partita, deve aver ottenuto esattamente 4 vittorie nelle precedenti 6 partite, e questo accade con probabilità (distribuzione binomiale) $(64) \cdot (4/7)^2 \cdot (3/7)^4$. Inoltre, deve forzatamente vincere alla settima partita, e questo accade con probabilità $3/7$. Quindi la probabilità cercata è $3/7 \cdot [(64) \cdot (4/7)^2 \cdot (3/7)^4] = (64) \cdot (4/7)^2 \cdot (3/7)^5$.
10. • Casi favorevoli: combinazioni di 3 su 4 (scelta di tre assi) x combinazioni di 2 su 36 (scelta di due carte fra le restanti del mazzo che non sono assi) = $4 \cdot (36 \cdot 35)/2$. Casi possibili: tutte le combinazioni di 5 su 40: $40!/(5!35!)$. La probabilità di pescare esattamente tre assi è $[4 \cdot (36 \cdot 35)/2]/[40!/(5!35!)] \cong 0,00383$.
- Poiché sono restare 35 carte di cui una sola è un asso, Matteo ottiene il poker con probabilità $1/35$.

11. Combinazioni di 2 su 3 x Combinazioni di 1 su 2 x Combinazioni di 2 su 4 = $3 \cdot 2 \cdot (4 \cdot 3/2) = 36$. Chiamo gli eventi: G=estrazione di una gialla, R=estrazione di una rossa, B=estrazione di una bianca. G_1 = esce una gialla alla prima estrazione, ecc ... Si ha $p(G_1) = 3/9$, $p(R_1) = 2/9$, $p(B_1) = 4/9$. La probabilità di estrarre una bianca alla seconda estrazione è:

$$p(B_2) = p(B_2 \cap G_1) + p(B_2 \cap R_1) + p(B_2 \cap B_1) =$$

(suddivido in una partizione di sottoeventi disgiunti)

$$p(G_1) \cdot p(B_2|G_1) + p(R_1) \cdot p(B_2|R_1) + p(B_1) \cdot p(B_2|B_1) =$$

(probabilità condizionata di eventi dipendenti, $3/9 \cdot 4/9 + 2/9 \cdot 4/10 + 4/9 \cdot 3/8 \cong 0.404$ poiché la prima estrazione modifica il contenuto dell'urna)

$$c - p(G_1|B_2) = p(B_2 \cap G_1)/p(B_2) = [p(G_1) \cdot p(G_1|B_2)]/p(B_2) = [3/9 \cdot 4/9]/[3/9 \cdot 4/9 + 2/9 \cdot 4/10 + 4/9 \cdot 3/8] \cong 0.37$$

12. La probabilità che una squadra vinca tutte le partite è $\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$. poiché è impossibile che più squadre vincano tutte le partite, possiamo moltiplicare tale risultato per il numero delle squadre. Pertanto la probabilità cercata è $4 \cdot \frac{1}{8} = \frac{1}{2}$.
13. La probabilità cercata è uguale alla probabilità che le due facce coperte diano somma $42 - 35 = 7$ (42 è la somma di tutti i punteggi dei due dadi). Qualsiasi sia la faccia coperta del primo dado, ce n'è una e una sola del secondo che tale che la somma sia 7. Quindi la probabilità cercata è $\frac{1}{6}$.
14. Fissati due dei tre colori, in ogni estrazione sarà possibile avere una probabilità pari a $\frac{2}{3}$ di estrarre una pallina di uno dei due colori. Quindi $(\frac{2}{3})^9$ sarà la probabilità che l'evento si verifichi per 9 volte di seguito. Qui però sono anche contati i casi in cui la pallina estratta è sempre dello stesso colore, per cui si dovrà sottrarre $2(\frac{1}{3})^9$. Questa differenza va moltiplicata per il numero di modi di fissare due colori a partire da un insieme di tre, ovvero $\binom{3}{2} = 3$, e pertanto sarà pari a: $3[(\frac{2}{3})^9 - 2(\frac{1}{3})^9] = \frac{2^9 - 2}{3^8} = \frac{510}{6561} = \frac{170}{2187}$.

15. Facendo 1, si ha già perso. Facendo 2, l'avversario deve per forza fare 2, probabilità del cui caso è $\frac{1}{36}$. Facendo 3, l'avversario deve fare 2 oppure 3, con probabilità $\frac{1}{36} + \frac{2}{36} = \frac{3}{36}$. Procedendo fino al caso 6, con probabilità tutte e note e facilmente calcolabili, si ottiene il risultato del problema $\frac{35}{216}$.

16. Per risolvere il problema è sufficiente osservare che le possibili configurazioni di pesci sui piatti, senza tenere conto dell'ordine, sono solamente 3: (1;1;1), (2;1;0) e (3;0;0).
Calcoliamo le probabilità di transizione da una configurazione ad un'altra:

- sia da (1;1;1) che da (3;0;0) si passa sempre alla configurazione (2;1;0);
- da (2;1;0) si può passare a (1;1;1) con probabilità $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$;
- da (2;1;0) si può passare a (3;0;0) con probabilità $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$;
- da (2;1;0) si può restare nella medesima configurazione con probabilità $1 \cdot \frac{1}{2}$.

I possibili cammini che in cinque mosse possono portare da (1;1;1) a (1;1;1) sono:

- (1;1;1) \rightarrow (2;1;0) \rightarrow (1;1;1) \rightarrow (2;1;0) \rightarrow (2;1;0) \rightarrow (1;1;1)
- (1;1;1) \rightarrow (2;1;0) \rightarrow (2;1;0) \rightarrow (1;1;1) \rightarrow (2;1;0) \rightarrow (1;1;1)
- (1;1;1) \rightarrow (2;1;0) \rightarrow (2;1;0) \rightarrow (2;1;0) \rightarrow (2;1;0) \rightarrow (1;1;1)
- (1;1;1) \rightarrow (2;1;0) \rightarrow (2;1;0) \rightarrow (3;0;0) \rightarrow (2;1;0) \rightarrow (1;1;1)
- (1;1;1) \rightarrow (2;1;0) \rightarrow (3;0;0) \rightarrow (2;1;0) \rightarrow (2;1;0) \rightarrow (1;1;1)

Calcolando le probabilità dei singoli percorsi e sommando si ottiene $\frac{5}{32}$.

6.5 Geometria

1. Con riferimento alla figura 6.6, si ha che:

$$area(ABCD) = area(OAB) - area(OCD) = \frac{50 \cdot 50}{2} - \frac{40 \cdot 40}{2} = 450 cm^2$$

L'area della regione in grigio è $\frac{1}{5}$ dell'area di $ABCD$, perché anche il segmento CD viene diviso in cinque parti uguali dalle semirette uscenti da O e i cinque trapezi in cui è suddiviso $ABCD$ hanno le stesse basi e la stessa altezza, e quindi sono equivalenti. L'area richiesta è quindi $90 cm^2$

2. Posto (figura 6.7) $AB = y$, dalla similitudine fra i triangoli AO_1T_1 e AO_2T_2 (triangoli rettangoli aventi un angolo in comune) si ha:

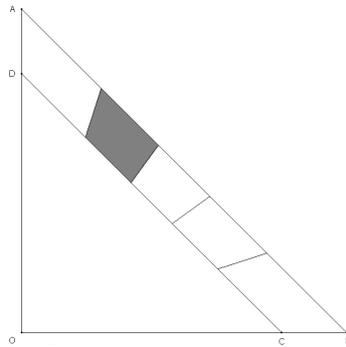
$$\frac{y+r}{r} = \frac{y+2r+x}{x}$$

cioè $x(y+r) = r(y+2r+x)$, da cui $xy = ry + 2r^2$ e infine $y = \frac{2r^2}{(x-r)}$.

Dalla similitudine tra i triangoli AO_1T_1 e AO_3T_3 si ha:

$$\frac{y+r}{r} = \frac{y+2r+2x+R}{R}$$

Figura 6.6:



cioè $R(y+r) = r(y+2r+2x+R)$. Sostituendo l'espressione per y ricavata dalla prima similitudine di ha che:

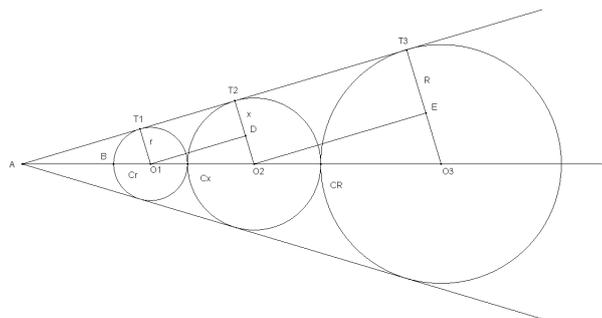
$$R \frac{2r^2}{x-r} + Rr = r \left(\frac{2r^2}{x-r} + 2(x+r) + R \right)$$

da cui segue che

$$\frac{rR}{x-r} = \left(\frac{r^2}{x-r} + (x+r) \right)$$

quindi si ottiene $Rr = r^2 + (x^2 - r^2)$ ed infine $x = \sqrt{Rr}$

Figura 6.7:



3. L'esagono che ha vertici nei centri dei sei cerchi periferici è regolare e ha lato 2. Pertanto la sua area è $6\sqrt{3}$. Ciascuna delle sei regioni dei cerchi piccoli esterna alle esagono ha area $\frac{2}{3}\pi$. Tenuto conto che l'area del cerchio grande è 9π , si ha che l'area della regione tratteggiata è

$$\frac{1}{6} \left[9\pi - 6 \cdot \frac{2}{3}\pi - 6\sqrt{3} \right] = \frac{5}{6}\pi - \sqrt{3}$$

4. Mentre la sfera ruota, il punto di contatto con i binari si muove su una circonferenza verticale di raggio $\sqrt{15^2 - 12^2}$ cm = 9 cm. La lunghezza di questa circonferenza è $2\pi \cdot 9$ cm = 18π cm.

5. La risposta è 72.

Infatti il tetraedro $ABPQ$ può essere pensato come una piramide di base ABP e altezza QM , dove M è il punto medio di AB . Se il lato del cubo è di 12, l'area di base sarà $\frac{144}{4} = 36$ e l'altezza sarà $\frac{12}{2} = 6$. Il volume del tetraedro sarà quindi $\frac{1}{3} \cdot 36 \cdot 6 = 72$

Elenchiamo qui alcune convenzioni del formalismo matematico utili per scrivere meglio le dimostrazioni e per comprendere gli scritti scientifici.

Logica

Con \mathcal{P} e \mathcal{Q} indichiamo generiche proposizioni, che possono essere vere o false.

- $\mathcal{P} \wedge \mathcal{Q}$: \mathcal{P} e \mathcal{Q} , vera solo se sono vere entrambe.
- $\mathcal{P} \vee \mathcal{Q}$: \mathcal{P} o \mathcal{Q} , vera solo se almeno una delle due è vera.
- $\neg \mathcal{P}$: non \mathcal{P} , vera solo se \mathcal{P} è falsa.
- $\mathcal{P} \rightarrow \mathcal{Q}$: \mathcal{P} implica \mathcal{Q} , vera a meno che \mathcal{P} sia vero e \mathcal{Q} falso. In una catena deduttiva, si preferisce usare la scrittura $\mathcal{P} \Rightarrow \mathcal{Q}$.
- $\mathcal{P} \leftrightarrow \mathcal{Q}$: \mathcal{P} se e solo se \mathcal{Q} , vera quando \mathcal{P} e \mathcal{Q} sono entrambe vere o entrambe false. In una catena deduttiva, si preferisce usare la scrittura $\mathcal{P} \Leftrightarrow \mathcal{Q}$.
- $\exists a : \mathcal{P}$: esiste a tale che \mathcal{P} , vera se per un qualche elemento a la proposizione \mathcal{P} è vera.
- $\exists! a : \mathcal{P}$: esiste un *unico* a tale che \mathcal{P} è vera.
- $\forall a : \mathcal{P}$: per ogni valore di a , vale \mathcal{P} .
- $::$: i due punti vanno tradotti come *tale che*.

Insiemi

Un insieme viene definito in termini di altri insiemi, di una proprietà o di un elenco di elementi. Insiemi noti sono \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , rispettivamente numeri naturali, interi, razionali, reali e complessi; oltre naturalmente all'insieme vuoto \emptyset , insieme che non contiene nessun elemento. Quando si definisce un insieme tramite condizioni o elenchi di elementi, si usano le parentesi graffe:

$$A = \{1, 2, 3\}, \quad B = \{a^2 : a \in A, a \text{ dispari}\} = \{1, 9\}$$

- $a \in A$: a appartiene ad A , per esempio $2 \in A$.

- $C \subseteq D$: C è un sottoinsieme di D . Se indichiamo $C \subset D$, allora vogliamo anche che $C \neq D$.
- $C \supseteq D$: C è un soprainsieme di D ; analogamente a prima $C \supset D$.
- $|A|$: la cardinalità di A , cioè il suo numero di elementi: $|A| = 3, |B| = 2$.
- $A \cup B$: A unione B , l'insieme che contiene gli elementi che sono in A o in B . Per esempio, $A \cup B = \{1, 2, 3, 9\}$.
- $A \cap B$: A intersezione B , l'insieme che contiene gli elementi che sono sia in A che in B . Per esempio, $A \cap B = \{1\}$.
- $A \setminus B$: A tranne B , l'insieme che contiene gli elementi in A e non in B . Per esempio, $A \setminus B = \{2, 3\}$.
- $A \times B$: A prodotto cartesiano B , l'insieme che contiene tutte le possibili coppie di elementi di cui il primo è in A e il secondo è in B . Per esempio, $A \times B = \{(1, 1), (1, 9), (2, 1), (2, 9), (3, 1), (3, 9)\}$
- $\mathcal{P}(A)$: l'insieme delle parti di A , cioè l'insieme che contiene tutti i possibili sottoinsiemi di A . Per esempio, $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Formule

- $a! = a \cdot (a-1) \cdot \dots \cdot 2 \cdot 1$: a fattoriale, cioè il prodotto dei numeri interi da 1 ad a .
- $\binom{a}{b} = \frac{a!}{b!(a-b)!}$: a su b , coefficiente binomiale.
- $\sum_{i=1}^n a_i = a_1 + a_2 + \dots + a_n$: sommatoria tra 1 e n dei numeri a_i .
- $\prod_{i=1}^n a_i = a_1 \cdot a_2 \cdot \dots \cdot a_n$: produttoria tra 1 e n dei numeri a_i .

Geometria

- $A \simeq B$: A congruente a B .
- $A \sim B$: A simile a B .
- $a \perp b$: a ortogonale a b .
- $a \parallel b$: a parallelo a b .

Miscellanea

- ∞ : infinito.
- $a|b$: a divide b , cioè b è multiplo di a .
- $a \equiv b \pmod{m}$: a congruo a b modulo m , cioè i due numeri hanno resti uguali se divisi per m .
- Negazioni: di molti simboli è prevista la versione sbarrata, che significa la negazione del simbolo originario: $\nexists a : \mathcal{P}, A \not\subseteq B, a \notin A, a \nmid b$ e così via.

Funzioni

- Si dice *funzione* e si indica con $f : A \rightarrow B$ una corrispondenza da un insieme A a un insieme B che sia *totale* (per ogni elemento $a \in A$ c'è un $b \in B$ associato) e *univocamente definita* (ogni elemento $a \in A$ non può avere associati due o più elementi di B).
- Si scrive $f(a) = b$ se ad a corrisponde b , e si dice che b è immagine di a e a è controimmagine di b .
- Si dice *grafico* di una funzione l'insieme dei punti $(a, b) \in A \times B$ con $f(a) = b$. Rigorosamente, in matematica una funzione è il suo grafico, e cioè una funzione è un insieme $f \subset A \times B$ che rifletta le proprietà di totalità e univocità.
- Si dice *iniettiva* una funzione tale per cui $a \neq b \Rightarrow f(a) \neq f(b)$.
- Si dice *suriettiva* una funzione tale per cui ogni elemento ha una controimmagine: $\forall b \exists a : f(a) = b$.
- Si dice *biunivoca* o *biiettiva* una funzione che è sia iniettiva che suriettiva. In tal caso si può definire la funzione inversa f^{-1} come: $f^{-1}(x) = y \Leftrightarrow f(y) = x$.
- Si indica con $f \circ g$ la funzione *composta* definita da $f \circ g(x) = f(g(x))$.
- Si dice che una funzione f è *crescente* (risp. *decescente*) se $x < y \Rightarrow f(x) \leq f(y)$ (risp. $f(x) \geq f(y)$). Si dice *strettamente* crescente o decrescente se le relazioni precedenti valgono con $<$, $>$ anzichè \leq , \geq .
- Si dice che una funzione è *concava* (risp. *convessa*) se il segmento che unisce due qualsiasi punti del suo grafico sta tutto al di sotto (risp. sopra) del grafico stesso.

Le *strategie euristiche* sono quell'insieme di idee, tecniche, suggerimenti e consigli che occorre tenere ben presenti per venire a capo di molti problemi. Sono una buona base di partenza per la risoluzione di un quesito e, al tempo stesso, un'ottima ultima spiaggia per chi non sa più "che pesci pigliare"

Riformulare il problema. Come regola generale, è importante sapere bene su cosa si sta lavorando. Qualsiasi cosa ci ritroviamo per le mani, conviene guardarla sotto tutti i punti di vista: se il problema è costituito da un polinomio (o un'espressione algebrica letterale), un'ottima idea è quella di scomporlo, poiché potrebbero emergere interessanti semplificazioni o relazioni. Allo stesso modo, se la nostra espressione è un polinomio già scomposto, proviamo ugualmente a svolgere i calcoli. Spesso la matematica è semplice, ma ben mimetizzata. Per fare questo è importante avere una buona conoscenza dei prodotti notevoli: non è raro vederli comparire in problemi delle Olimpiadi di Matematica.

Provare i casi semplici. Per chiarire meglio come si comporti l'oggetto matematico che stiamo esaminando, conviene sempre prima provare un certo numero di casi semplici, per rendersi conto di come si comporti il problema al variare delle condizioni di partenza. Spesso alcune proprietà si possono dedurre estrapolando il comportamento del problema a partire dai casi semplici che sono stati esaminati. Risolvere un problema a tentativi non è certamente incoraggiato, ma talvolta può essere una strategia vincente: di certo i tentativi non fanno male, e spesso permettono di escludere casi altrimenti non facilmente "visibili".

Induzione. Se dobbiamo dimostrare una certa proprietà o relazione che coinvolge i numeri naturali, la primissima cosa da fare è tentare di farlo con il principio di induzione. Questo non significa che funzioni sempre, ma solitamente è una buona strategia.

Assurdo. Se dobbiamo dimostrare che una qualche situazione è impossibile, a seconda del contesto potrebbe essere una buona idea cercare qualche invariante che non viene rispettato, sostituire un'equazione con una congruenza più semplice ma ugualmente impossibile, o comunque provare a ragionare per assurdo.

Problemi di velocità. Nel caso ci siano problemi con punti che si muovono a velocità diverse è sempre opportuno, per chiarire le idee (se non addirittura per risolvere il problema) fare un grafico spazio-tempo o velocità-tempo, a seconda del problema. Questi grafici in particolare sono molto comodi quando si parla di accelerazioni costanti perché così si

ottengono delle rette che chiariscono molto il problema (punti di incontro, di sorpasso, etc...)

Figure. Nel caso di problemi geometrici, è fondamentale realizzare una figura sufficientemente grande e segnare con un colore diverso tutto ciò che si conosce sul problema: questo permette di capire più rapidamente cos'altro si potrebbe sapere e, di conseguenza, capire quale sia la vera incognita del problema. Se la figura dipende dalla scelta di alcuni oggetti (solitamente ampiezze di angoli o lunghezze di segmenti), il consiglio è di realizzare più figure, per poi scegliere quella che si adatta meglio a successive costruzioni o quella che rappresente maggiormente il problema.

Geometria solida. In particolare, nei problemi di geometria solida, la maggiore difficoltà sta proprio nel visualizzare una buona figura. Conviene quindi rappresentare il problema più volte, visto da diverse angolazioni; di modo da chiarire il più possibile su cosa si sta lavorando.

Calcolo tutto. Sempre nei problemi geometrici, una strategia utile (detta del *calcolo tutto*) consiste nell'individuare quelle lunghezze, o angoli, dati i quali la figura è completamente determinata, indicare la loro lunghezza (o ampiezza) con delle incognite x, y, \dots e poi tentare di calcolare tutti gli altri angoli o lunghezze in funzione di quelle incognite iniziali, segnandoli ogni volta sulla figura. Se quindi l'obiettivo era dimostrare una qualche uguaglianza tra angoli o segmenti, usando opportuni teoremi l'uguaglianza si può tradurre in un'equazione algebrica che (forse) è possibile risolvere.

Ultima spiaggia. Nell'eventualità poi che un problema geometrico sia davvero complesso, una strategia euristica che risulta spesso efficace, sia pure poco "seria", è quella di *tracciare, a caso, tutte le circonferenze che si possono tracciare*, cercando di trovarne qualcuna per cui passino il più punti possibile. Spesso una dimostrazione passa per qualche relazione tra angoli o lati, e l'uso delle circonferenze è, se non necessario, particolarmente semplificato.

Se poi non ci viene proprio in mente come risolvere un problema geometrico, una sorta di ultima spiaggia può essere... cominciare ad usare il goniometro. Qualcosa (si spera) ne verrà fuori: in particolare se il problema è a risposta numerica su un angolo, l'uso del goniometro su una buona figura può fornire una risposta quasi esatta. Con occhio critico, approssimate il valore ottenuto alla più vicina frazione di 180° : per esempio, se ottenete 58° , conviene scrivere 60° .

Se ancora non riuscite a risolvere il problema, una strategia geometrica di ultima spiaggia (che raramente è utile) e quella di impostare il problema in maniera analitica.

Tabelle riassuntive

Riportiamo qui alcune tabelle sugli argomenti precedenti per una rapida consultazione in caso di necessità.

Logica e Matematizzazione

Congiunzione logica \wedge	serve personale che sappia il francese e l'inglese.
Disgiunzione inclusiva \vee	serve personale che sappia il francese o l'inglese.
Disgiunzione esclusiva $\dot{\vee}$	o mangi la minestra o salti la finestra.
Negazione \neg	il numero 3 non è pari.
Implicazione \Rightarrow	se piove allora prendo l'ombrello.
Coimplicazione \Leftrightarrow	piove se e solo se cade acqua dal cielo.

Teoria dei Numeri

2	$x \equiv$ ultime n cifre di $x \pmod{2^n}$
3	$x \equiv$ somma delle sue cifre $\pmod{3}$ o 9
5	$x \equiv$ ultime n cifre di $x \pmod{5^n}$
11	$x \equiv$ somma a segno alterno delle sue cifre $\pmod{11}$
n	$a = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r} : a n \Leftrightarrow p_1^{\alpha_1} n, \dots, p_r^{\alpha_r} n$

Somma	$(a + b) \bmod m = a \bmod m + b \bmod m \pmod{m}$
Prodotto	$(a \cdot b) \bmod m = (a \bmod m) \cdot (b \bmod m) \pmod{m}$
Potenza	$a^n \bmod m = (a \bmod m)^{n \bmod \text{ord}(m)} \pmod{m}$

Algebra

Progressioni aritmetiche	$a_n = a_{n-1} + d$ <p>Generico termine: $a_r = a_s + (r - s)d$</p> <p>Somma dei termini da s a r: $S = \frac{1}{2}(a_r + a_s)(r - s + 1)$</p>
Progressioni geometriche	$a_n = k \cdot a_{n-1}$ <p>Generico termine: $a_r = k^{(r-s)}a_s$</p> <p>Somma dei termini da s a r: $S = a_r \frac{k^{(s-r+1)} - 1}{k - 1}$</p> <p>Prodotto dei termini da a_r a a_s: $P = \sqrt{(a_r \cdot a_s)^{(r-s+1)}}$</p>

Relazioni tra radici e coefficienti	$-a_{n-1} = \sum_{1 \leq i \leq n} \lambda_i$ $a_{n-2} = \sum_{1 \leq i < j \leq n} \lambda_i \cdot \lambda_j$ $-a_{n-3} = \sum_{1 \leq i < j < k \leq n} \lambda_i \cdot \lambda_j \cdot \lambda_k$ \vdots $(-1)^n a_0 = \lambda_1 \cdot \lambda_2 \cdot \dots \cdot \lambda_n$
--	--

Media aritmetica	$AM = \frac{a_1 + \dots + a_n}{n}$
Media geometrica	$GM = \sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n}$
Media armonica	$HM = \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n}}$
Disuglianza tra le medie	$HM \leq GM \leq AM$

Combinatoria

Fattoriale	$n! = n \cdot (n - 1) \cdot (n - 2) \cdot \dots \cdot 2 \cdot 1$
Coefficiente binomiale	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$
Regole di calcolo	$\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}$ $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$ $\binom{n}{k} = \binom{n}{n-k}$ $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ $\sum_{k=0}^n \binom{n}{k} = 2^n$
Binomio di Newton	$(a + b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \dots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n$ $= \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$

Permutazioni semplici modi di disporre n oggetti in n posti	$P(n) = n!$
Permutazioni con ripetizione modi di disporre n oggetti in n posti sapendo che k_1 sono uguali ad un oggetto $a_1, \dots,$ k_m sono uguali ad un oggetto a_m	$P(n) = \frac{n!}{k_1! \cdot k_2! \cdot \dots \cdot k_m!}$
Disposizioni semplici modi di scegliere k oggetti da un gruppo di n tenendo conto dell'ordine: $(a, b, c) \neq (b, a, c)$	$D_{n,k} = n \cdot (n-1) \cdot \dots \cdot (n-(k-1)) = \frac{n!}{(n-k)!}$
Disposizioni con ripetizione modi di prendere k oggetti di n tipi sapendo che ogni elemento può essere ripetuto più volte	$D'_{n,k} = n^k$
Combinazioni semplici modi di scegliere k oggetti da un gruppo di n non contando l'ordine: $(a, b, c) \equiv (b, a, c)$	$C_{n,k} = D_{n,k} / P_k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$
Combinazioni con ripetizione modi di scegliere k oggetti di n tipi con elementi ripetuti non contando l'ordine: $(a, a, b) \equiv (a, b, a)$	$C'_{n,k} = \binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}$

Probabilità del <i>not</i>	$P(\text{non } A) = 1 - P(A)$
Probabilità dell'<i>or</i>	$P(A \text{ o } B) = P(A) + P(B) - P(A \text{ e } B)$
Probabilità dell'<i>and</i>	$P(A \text{ e } B) = P(A) \cdot P(B \text{ sapendo che } A \text{ è avvenuto})$

Geometria

Triangolo	$A = \frac{1}{2} \cdot b \cdot h$
Parallelogramma	$A = b \cdot h$
Trapezio	$A = \frac{1}{2} \cdot h \cdot (B + b)$
Rombo	$A = \frac{1}{2} \cdot d_1 \cdot d_2$
Poligono regolare di n lati	$A = \frac{1}{2} \cdot n \cdot l \cdot a$ dove a sta per apotema
Cerchio	$A = \pi r^2$
Settore circolare	$A = \frac{\alpha}{360} \cdot \pi r^2$ dove α è espresso in gradi
Prisma	$V = A_b \cdot h$
Piramide retta	$V = \frac{1}{3} \cdot A_b \cdot h$
Cilindro	$V = \pi r^2 h$
Cono	$V = \frac{1}{3} \pi r^2 h$
Sfera	$V = \frac{4}{3} \pi r^3$
Raggio della circonferenza circoscritta	$R = \frac{abc}{4A}$
Raggio della circonferenza inscritta	$r = \frac{A}{p}$
Formula di Erone	$A = \sqrt{p(p-a)(p-b)(p-c)}$
Formula di Eulero	$F - S + V = 2$

Bibliografia

- [1] M. Gobbino: *Schede Olimpiche — Per la preparazione alle Olimpiadi della Matematica*, Edizioni Cremonese (2005)
- [2] F. Conti, M. Barsanti, T. Franzoni: *Le Olimpiadi della Matematica — Problemi dalle gare italiane dal 1988 al 1994*, Zanichelli (1994)
- [3] F. Conti, M. Barsanti, C. De Lellis, T. Franzoni: *Le Olimpiadi della Matematica — Problemi dalle gare italiane dal 1995 al 2001*, Zanichelli (2002)
- [4] <http://olimpiadi.dm.unibo.it/> , sito ufficiale delle Olimpiadi della Matematica