Teoria di Base

a.k.a. guida (in)completa per Archimede e EGMOcamp

Barbara Catino - Filippo Gargiulo

Ottobre 2024

Introduzione

Questo documento è una rassegna di teoria utile per risolvere i problemi di Archimede, Febbraio e dell'ammissione all'EGMOcamp. **Questo non è da intendersi come un "libro di testo" in cui la teoria viene introdotta in modo sistematico**, giustificando e dimostrando ogni lemma, facendo molti esempi e fornendo una lista di esercizi per praticare gli argomenti. L'intento era quello di scrivere un insieme di teoria "quick and dirty" che sarebbe potuta risultare utile per ripassare ciò che si aveva già studiato poco prima di una gara, o per entrare a conoscenza di piccoli fatti di teoria (utili ma assolutamente non necessari). Nonostante una delle intenzioni fosse anche quella di dare a chi si approccia per la prima volta a questo mondo una sorta di mappa, per orientarsi e rendersi conto della dimensione delle cose che già sa o che ancora non sa, il lettore alle prime armi non si deve spaventare. Come è già stato detto, **la matematica olimpica si basa sul sapersi arrangiare in situazioni sconosciute**; che senso avrebbe ciò se si potesse studiare la teoria che sta dietro ad ogni possibile problema e spegnere completamente il cervello?
Sapere la teoria è sempre secondario al saper ragionare, e per quanto **la teoria esposta qui** si possa considerare "di base" **non va intesa come "la teoria che è indispensabile sapere per poter fare le olimpiadi della matematica"**. Una cosa del genere non esiste e speriamo continui a non esistere ancora a lungo. Questa è unicamente della teoria che può risultare utile, facilmente sostituibile con una sufficiente dose di astuzia e buona volontà. Questa teoria è da considerarsi invece "di base" nel senso che è quella teoria che uno studente veterano, ormai abituato a risolvere problemi di stile olimpico, dovrebbe conoscere (o almeno saper dimostrare essere vera) a grandi linee; non necessariamente perchè l'ha studiata sistematicamente nel passato, anzi, di solito è perchè ha risolto **problemi che richiedevano di dedurre alcune di queste cose da zero**. Incoraggiamo quindi chiunque si sentisse in vena di esercizio, a dimostrare i lemmi e teoremi qui presentati.

Si ringrazia Evan Chen per il template LaTeX.

Indice

§1 Teoria dei numeri

§1.1 Divisibilità

Definizione 1.1. Divisione euclidea. Siano a e b due interi, con $a \neq 0$. Allora esistono due numeri interi q e r, tali che:
(i) $b = aq + r$,
(ii) $0 \leq r < |a|$. Inoltre q ed r sono unici.

Definizione 1.2. Divisore. Se nell'equazione sopra $r = 0$, si dice che a è un divisore di b e scriviamo $a \mid b$.

Definizione 1.3. Massimo comune divisore. Dati n interi positivi $a_1, \ldots, a_n$, si dice massimo comun divisore di $a_1, \ldots a_n$, e si indica con la notazione MCD$(a_1, \ldots a_n)$, il più grande intero positivo che divide tutti gli a_i. In inglese si indica con GCD (che sta per "greatest common divisor").

Definizione 1.4. Dati n interi positivi $a_1, \ldots a_n$ chiamiamo Minimo Comune Multiplo e scriviamo mcm$(a_1, \ldots a_n)$ il minimo numero diviso da tutti gli a_i. In inglese si indica con LCM (che sta per "least common multiple").

Definizione 1.5. Definiamo due numeri $a, b \in \mathbb{N}$ *coprimi* se e solo se MCD$(a, b) = 1$

Definizione 1.6. Definiamo *primo* un numero che ha come divisori solo 1 e se stesso. Ogni primo è ovviamente coprimo con ogni altro numero minore di se stesso e maggiore di 0. Definiamo $\mathbb{P}$ l'insieme che contiene tutti e soli i primi.

Un cruciale risultato che di solito si tratta alle medie, è il seguente teorema:

Teorema 1.7 (Fondamentale dell'Aritmetica)

Ogni numero $n \in \mathbb{N}$ può essere scritto in modo univoco come prodotto di numeri primi, cioè:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_k^{\alpha_k}$$

Dove k è un certo numero intero, $p_i \in \mathbb{P}$ e $\alpha_i \in \mathbb{Z}$ (con $0 < i \leq k \in \mathbb{N}$).

Quando un numero è scritto in quella forma si dice essere "fattorizzato". Fattorizzare i numeri è in generale una buona idea per risolvere equazioni diofantee.

Dal teorema prececente deriva il seguente utile lemmino, che facilita spesso i conti:

Lemma 1.8 (Numero di divisori)

Sia n un numero intero fattorizzato usando la notazione del precedente teorema, allora il numero di divisori interi positivi di n è:

$$(\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \ldots (\alpha_k + 1)$$

La dimostrazione di questo fatto è un esercizio di combinatoria molto costruttivo (fondamentalmente un'applicazione di 4.3) ed è quindi fortemente consigliato provare a dimostrarlo da soli.

Lemma 1.9

Se abbiamo un primo $p \in \mathbb{P}$ e due numeri $a, b \in \mathbb{N}$, allora se vale

$$p \mid ab$$

vale anche $p \mid a$ o $p \mid b$ (potenzialmente entrambe).

Questo potrà sembrare un risultato stupido, ma è alla base di molti teoremi e importanti strategie risolutive, si pensi ad esempio alla risoluzione dell'equazione $ab = 90$ con $a, b \in \mathbb{N}$. Parliamo ora un po' delle proprietà di mcm e MCD:

Lemma 1.10

Dati due interi $a, b \in \mathbb{N}$, abbiamo che:

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

Lemma 1.11

Dati $a, b \in \mathbb{N}$ abbiamo che:

$$\text{MCD}(a, b) = \text{MCD}(a - kb, b)$$

Per un arbitrario $k \in \mathbb{Z}$.

Il lemma precedente giustifica il prossimo importante risultato

Algoritmo 1.12 (di Euclide) — Supponiamo di voler calcolare l'MCD tra $a, b \in \mathbb{N}$. Allora possiamo dividere a per b e ottenere:

$$\begin{aligned} a = bq_1 + r_1 &\iff a - bq_1 = r_1 \qquad \text{MCD}(a, b) = \text{MCD}(b, r_1) \\ b = r_1q_2 + r_2 &\iff b - r_1q_2 = r_2 \qquad \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2) \\ &\vdots \\ r_k = q_{k+2}r_{k+1} &\iff r_k - q_{k+2}r_{k+1} = 0 \qquad \text{MCD}(r_{k+1}, r_k) = \text{MCD}(r_{k+1}, 0) = r_{k+1} \end{aligned}$$

Cioè ci basta continuare a dividere i resti tra di loro, finchè non arriviamo a 0, a quel punto l'MCD sarà l'ultimo resto non 0 della catena di divisioni.

"Riavvolgendo al contrario" il precedente algoritmo possiamo facilmente arrivare al seguente risultato:

Teorema 1.13 (Bezóut)

Siano $a, b \in \mathbb{N}$, allora è sempre possibile trovare due numeri $m_0, n_0 \in \mathbb{Z}$ tali che:

$$m_0a + n_0b = \text{MCD}(a, b)$$

Finiamo questa sezione con un breve approfondimento sulle basi di numerazione:

Definizione 1.14. La scrittura: $n = \overline{a_k a_{k-1} a_{k-2} a_{k-3} \dots a_0}$ significa che il numero n è formato dalle cifre a_0, a_1, a_2 $\dots a_k$ in quell'ordine (ovviamente in base 10 gli a_i sono

compresi tra 0 e 9 inclusi). Per esempio per $n = 456$, $a_2 = 4$, $a_1 = 5$, $a_0 = 6$.

Ora, il nostro sistema di numerazione usuale è la base 10, il che significa che ci sono 10 cifre, e che scrivere un numero con le cifre a_0, a_1, a_2, $\ldots a_k$ significa:

$$n = \overline{a_k a_{k-1} a_{k-2} \ldots a_0} = a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots + 10^k a_k$$

Non è raro tuttavia incontrare problemi che chiedano di utilizzare basi di numerazione diverse dal 10, quindi la seguente definizione.

Definizione 1.15. Un numero n è rappresentato in base b dalle cifre a_0, a_1, a_2, $\ldots a_k$ (con $0 \leq a_i < b$ per ogni i compreso tra 0 e k inclusi) se e solo se:

$$n = (\overline{a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_0})_b = a_0 + ba_1 + b^2 a_2 + b^3 a_3 + b^4 a_4 + \cdots + b^k a_k$$

Utilizzare la definizione sopra di solito basta per avviarsi alla risoluzione di tutti i quesiti che coinvolgono le basi di numerazione.

§1.2 Aritmetica modulare

Definizione 1.16. Si dice che due interi a, b sono congrui modulo (più semplicemente mod.) m, e si scrive $a \equiv b\ (m)$, se a e b, divisi per m, danno lo stesso resto. L'insieme di tutti gli interi congruenti a due a due mod. m forma una classe di congruenza, che viene indicata con il più piccolo intero maggiore o uguale a 0 nella classe.

> **Osservazione 1.17.** Utilizzando la divisione euclidea come definita al paragrafo precedente possiamo dimostrare che le seguenti tre proposizioni sono logicamente equivalenti:
>
> - $a \equiv b \pmod{n}$
> - $n \mid a - b$
> - a e b hanno lo stesso resto nella divisione per n.

Questa relazione è fondamentale per la risoluzione di molti problemi di teoria dei numeri. Per esempio nelle equazioni diofantee è spesso molto utile invocare la proprietà per cui $a \equiv b \pmod{n} \iff n \mid a - b$; infatti se $a = b$ allora $a - b = 0$, e grazie al fatto che $n \mid 0$ possiamo dimostrare il seguente fatto:

Fatto 1.18. Date due espressioni intere a e b, abbiamo sempre:

$$a = b \implies a \equiv b \pmod{n}$$

E quindi spesso utile "analizzare mod n" un'equazione diofantea per trovare contraddizioni o condizioni interessanti grazie alle semplificazioni che di solito è molto facile fare mod n. Vediamo ora come si possono fare queste fantomatiche semplificazioni:

Lemma 1.19 (Principi di Equivalenza $\mod n$)

Siano $a, b, c, d, n \in \mathbb{Z}$, allora se valgono:

$$a \equiv c \pmod{n}$$
$$b \equiv d \pmod{n}$$

Valgono anche le seguenti:

$$a \cdot b \equiv c \cdot d \pmod{n}$$
$$a \pm b \equiv c \pm d \pmod{n}$$

Lemma 1.20 (Divisione $\mod n$)

Siano $a, b, c, n \in \mathbb{Z}$, allora se vale:

$$ac \equiv bc \pmod{n}$$

Vale anche:

$$a \equiv b \pmod{\frac{n}{\mathrm{MCD}(n, c)}}$$

Corollario 1.21 (Inverso $\mod p$)

Da sopra si evince che, dato che un primo è sempre coprimo con tutti gli altri numeri minori di se stesso e maggiori di 0, preso un primo $p \in \mathbb{P}$ esiste sempre l'inverso mod p. Ovvero per ogni intero $a \not\equiv 0 \pmod{p}$ esiste sempre un intero a^{-1} tale che:

$$a \cdot a^{-1} \equiv 1 \pmod{p}$$

Inoltre si può dimostrare che un tale a^{-1} è sempre unico, una volta scelto a.

"I primi sono belli" come affermò un noto Ex-Studente del Volta.[1] I precedenti tre risultati, permettono di semplificare grandemente espressioni numeriche e non. Infatti grazie al lemma 1.19 abbiamo:

Fatto 1.22. Se $a \equiv b \pmod{n}$ allora $a - nk \equiv b - 0 \equiv b \pmod{n}$ per un arbitrario $k \in \mathbb{Z}$.

Fantastico, adesso abbiamo un modo per liberarci velocemente di somme e prodotti. E con gli esponenti? E con cose più esotiche? Come facciamo?
Esistono alcuni utili teoremi che permettono di semplificare gli esponenti e i fattoriali modulo p primo. Bisogna dire però che **raramente questi sono utili nel contesto di una gara di Archimede, una gara di Febbraio o un Test di ammissione EGMOcamp**. A Cesenatico possono risultare utili per gli ultimi problemi, ma rimangono comunque **teoremi molto avanzati, le cui dimostrazioni risultano particolarmente più difficili** rispetto a tutti gli altri qui trattati. Li includiamo qui per completezza, ma tenete presente che probabilmente il concorrente medio di Cesenatico non li conosce e non li sa dimostrare. Traetene le vostre conclusioni.

[1] Edoardo Balistri

Teorema 1.23 (Piccolo Teorema di Fermat)

Sia $p \in \mathbb{P}$ e $a \in \mathbb{N}$, allora vale sempre:

$$a^p \equiv a \pmod{p}$$

Teorema 1.24 (Wilson)

Sia $p \in \mathbb{P}$, allora vale sempre:

$$(p-1)! \equiv -1 \pmod{p}$$

per la definizione di ! si rimanda a 4.7.

Ma questo ancora non basta, che ne è dei numeri che non sono primi? Come facciamo a semplificare espressioni in modulo arbitrario?
Spesso in teoria dei numeri accade che i problemi si prestino a risolversi prima per i numeri primi (o per le potenze di numeri primi), e poi siano facilmente generalizzabili "mettendo insieme" i risultati e ottenendo numeri composti. Detta così questa strategia ci dice poco, il prossimo teorema però, ne è un esempio lampante:

Teorema 1.25 (Teorema Cinese del Resto/Chinese Remainder Theorem/CRT/TCR)

Siano, $a, b, n, p, q \in \mathbb{N}$ e siano $pq = n$ con p, q coprimi. Si vede facilmente allora come la congruenza $a \equiv b \pmod{n}$ sia equivalente al seguente sistema di congruenze:

$$\begin{cases} a \equiv b \pmod{p} \\ a \equiv b \pmod{q} \end{cases}$$

cioè, la congruenza $a \equiv b \pmod{n}$ è vera se e solo se è sono soddisfatte contemporaneamente tutte le congruenze del sistema sopra.

Questo significa che in un modo o nell'altro, possiamo sempre ricondurci al caso n primo, o al n limite potenza di un primo. Generalizziamo ulteriormente alcuni risultati visti sopra:

Lemma 1.26 (Inverso $\bmod n$)

Se $n \in \mathbb{N}$ è un generico numero naturale, e $a \leq n \in \mathbb{N}$, allora esiste sempre ed è unico un numero $a^{-1} \leq n \in \mathbb{N}$ tale che

$$a \cdot a^{-1} \equiv 1 \pmod{n}$$

solo se a è coprimo con n.

Per il prossimo teorema vale l'avvertimento dato sopra, se possibile ancora più rimarcato per la sua difficoltà e relativa inutilità.

Teorema 1.27 (Eulero-Fermat)

Sia $n \in \mathbb{N}$, e sia $\varphi(n)$ la funzione che denota il numero di interi minori o uguali a n e coprimi con n. Per ogni $a \in \mathbb{N}$ coprimo con n vale la seguente relazione:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

§2 Geometria

La geometria non è un reato

Renato Zero, il triangolo.

§2.1 Fatti di angoli noti

Segue uno spam di fatti di geometria presumibilmente noti:

Fatto 2.1. Due angoli opposti al vertice sono congruenti.

Fatto 2.2. Due angoli adiacenti sono supplementari (la loro somma è sempre 180°).

Fatto 2.3. La somma degli angoli interni di un triangolo sul piano è 180°.

Fatto 2.4. La somma degli angoli interni di un poligono a n lati è sempre uguale a $180(n-2)$ gradi.

Fatto 2.5. La somma degli angoli esterni di un poligono è sempre uguale a 180°.

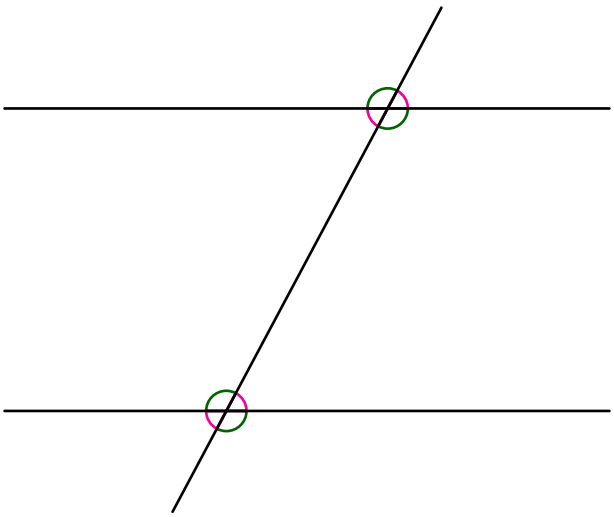
Fatto 2.6. Presa una retta r e un punto P esiste sempre ed è unica una retta passante per P e parallela a r.

Fatto 2.7. Presa una retta r e un punto P esiste sempre ed è unica una retta passante per P e perpendicolare a r.

Fatto 2.8. Se due angoli di un triangolo sono uguali allora anche i lati a loro opposti lo sono.

Fatto 2.9. L'angolo esterno in un triangolo è uguale alla somma dei due angoli a lui non adiacenti.

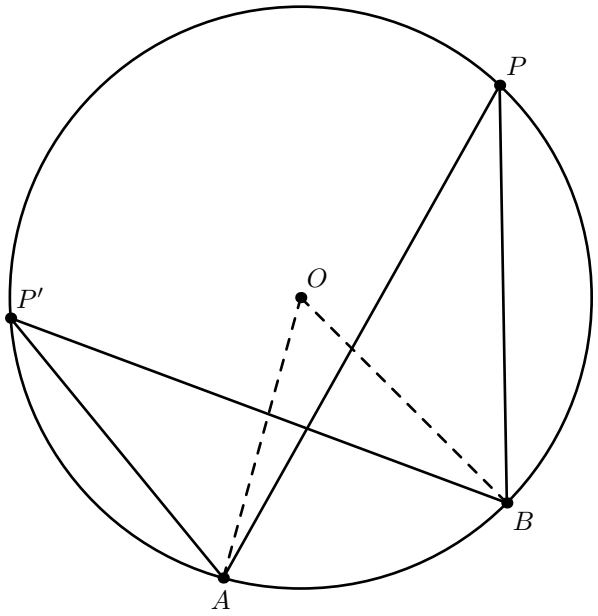
Fatto 2.10. Prese due rette parallele tagliate da una trasversale come in figura, gli angoli colorati dello stesso colore in figura sono uguali:



Inoltre questa cosa si può invertire (se due angoli non opposti al vertice tra quelli sono uguali, allora le rette sono parallele).

§2.2 Circonferenze e "Angle Chasing"

Prendiamo una circonferenza e due punti A e B su di essa



Questi due punti dividono la circonferenza in due archi.

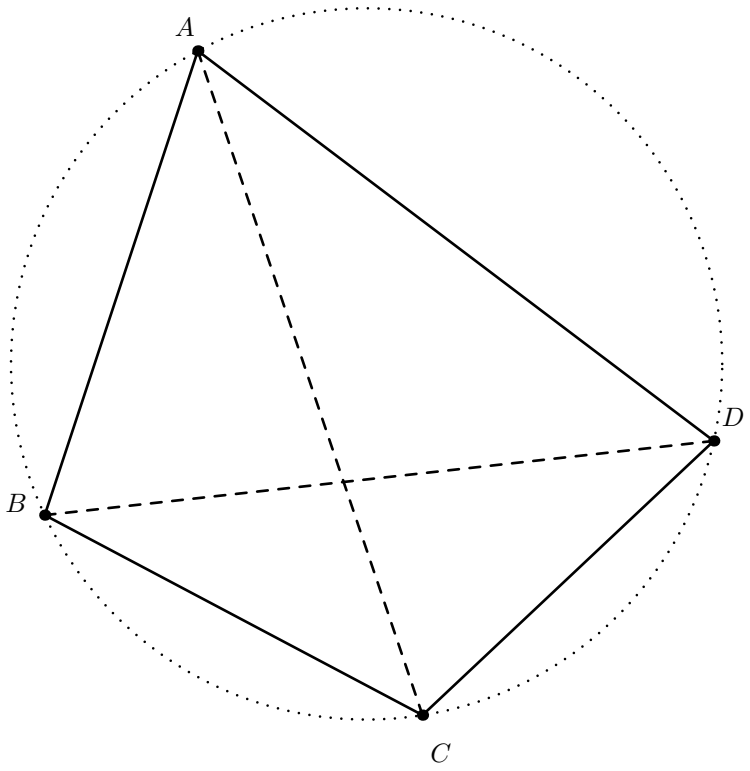
Definizione 2.11. Presi due punti P e P' su uno dei due archi prima definiti, diciamo che gli angoli $\angle BPA$ e $\angle BP'A$ sono angoli *alla circonferenza* che *insistono* sullo stesso arco (l'arco AB per la precisione). Inoltre si dimostra che due angoli alla circonferenza che insistono sullo stesso arco sono sempre uguali, cioè $\angle BPA = \angle BP'A$ per ogni scelta di P e P' su uno stesso arco.

> **Osservazione 2.12.** Il fatto enunciato sopra funziona anche se il punto P coincide con uno dei due punti A oppure B. Se infatti $P \equiv A$ (P coincide con A) l'angolo che insiste sull'arco AB sarà quello avente come lati la retta AB e la retta passante per A e tangente alla circonferenza.

Un'altra importante proprietà degli angoli che insistono su un arco AB è che, chiamato O il centro della circonferenza abbiamo:

Definizione 2.13. Diciamo che l'angolo *al centro* $\angle AOB$ convesso *insiste* sull'arco minore delineato da AB. Si dimostra che preso uno stesso arco, l'angolo al centro che insiste su di esso è sempre il doppio dell'angolo alla circonferenza che insiste su di esso, cioè $\angle BAO = 2 \times \angle BPA$.

Definizione 2.14. Diciamo che un quadrilatero $ABCD$ è ciclico, e scriviamo $ABCD\,cyc$ quando esiste una circonferenza che passa per tutti i suoi quattro vertici, come in figura.



Osservazione 2.15. Per quanto detto prima sugli angoli al centro e alla circonferenza, le seguenti informazioni e l'informazione $ABCD\,cyc$ sono tutte equivalenti:

- $\angle CAB = \angle CDB$
- $\angle BCA = \angle BDA$
- $\angle ABD = \angle ACD$
- $\angle DAC = \angle DBC$
- $\angle DAB + \angle BCD = 180°$
- $\angle ABC + \angle CDA = 180°$

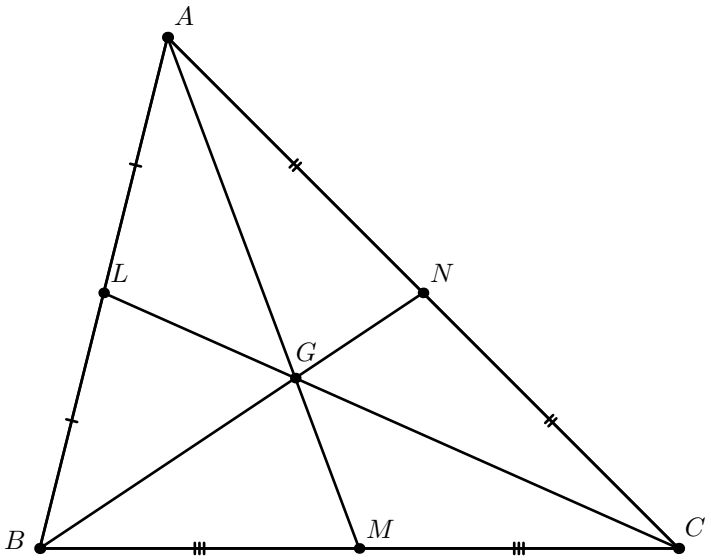
Sapendo tutto cio che è stato illustrato in questa sezione e in quella precedente è possibile fare il cosiddetto "Angle Chasing" ("Andar per Angoli"/"Inseguire gli Angoli"), cioè calcolare il valore di alcuni angoli del problema in funzione di altri angoli per dimostrare proprietà utili alla risoluzione del problema. Questa tecnica unita all'analogo "Length Chasing" permette di risolvere la stragrande maggioranza dei problemi di geometria, dagli archimede più semplici ai Cese5/6 fino ai primi problemi delle shortlist delle IMO. Dunque è essenziale dominare questa strategia risolutiva per diventare bravi in Geometria (Olimpica).

§2.3 Punti Notevoli e configurazioni

Il grosso della teoria di geometria oltre un certo punto consiste in configurazioni geometriche da "imparare a memoria". Qui vogliamo riassumere le prime e più semplici che si imparano risolvendo problemi di geometria.
Sia per quanto riguarda il circocentro che per l'incentro e l'ortocentro, trovare le espressioni di tutti gli angoli nella figura in funzione di $\angle CAB$, $\angle ABC$ e $\angle BCA$ è molto semplice, e per questo incoraggiamo caldamente i lettori a cimentarsi nell'impresa.
Cogliamo anche l'occasione per introdurre un po' di "notazione standard" per i triangoli:

- Di solito il punto in alto è A, e si procede a dare i nomi agli altri due in senso antiorario.
- Di solito gli angoli del triangolo si indicano con le seguenti lettere greche: $\angle CAB = \alpha$, $\angle ABC = \beta$, $\angle BCA = \gamma$
- Di solito i lati del triangolo sono chiamati: $BC = a$, $AC = b$, $AB = c$.
- Di solito il raggio della circonferenza circoscritta è indicato come R, quello della circonferenza inscritta invece come r.

§2.3.1 Baricentro



Definizione 2.16. Chiamiamo A-Mediana di un triangolo la retta passante per il vertice A e per il punto medio del lato opposto BC. Analogamente definiamo la B-Mediana e la C-Mediana

In figura abbiamo chiamato M, N, L i punti medi dei lati BC, AC, AB.

Definizione 2.17. Chiamiamo Baricentro di un triangolo l'intersezione delle sue mediane. Si può dimostrare che il baricentro esiste sempre ed è unico.

Il baricentro di un triangolo ha numerose proprietà interessanti, ne elenchiamo alcune:

Lemma 2.18 (Centro di massa)

Se ipotizziamo di costruire un triangolo di massa uniforme come quello in figura, di vertici A, B e C, il centro di massa di questo oggetto risulta essere proprio il baricentro del triangolo ABC.

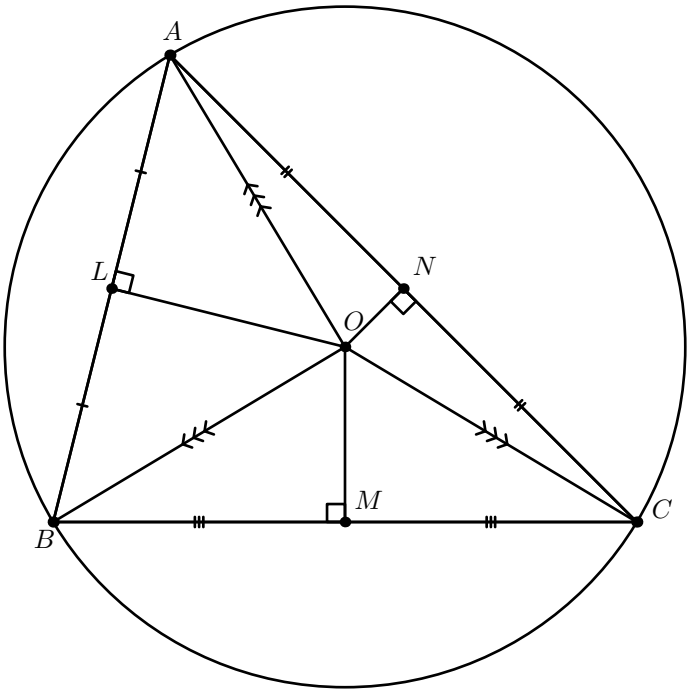
Lemma 2.19 (Teorema del Baricentro)

Il baricentro taglia le mediane in segmenti in rapporto $2 : 1$, ovvero usando la notazione della figura abbiamo $AG = 2GM$, $CG = 2GL$ e $BG = 2GN$.

Lemma 2.20 (Teorema dei punti medi)

Usando la notazione della figura abbiamo $LN||BC$, $MN||AB$ e $ML||AC$. Questo segue facilmente da 2.39.

§2.3.2 Circocentro



Definizione 2.21. Chiamiamo *asse* di un segmento la retta perpendicolare a questo e passante per il suo punto medio. Si può dimostrare che l'asse di un segmento è formato da tutti e soli i punti equidistanti dai suoi estremi (nel gergo si dice che l'asse è il luogo dei punti equidistanti dai due punti che sono estremi del segmento).

Definizione 2.22. Diciamo *circocentro* di un triangolo ABC il centro della circonferenza passante per A, B, C.

Corollario 2.23

Gli assi dei lati AB, BC, CA di un triangolo ABC concorrono in un punto che coincide con il circocentro del triangolo, che quindi esiste sempre ed è unico.

§2.3.3 Incentro

Definizione 2.24. Chiamiamo A-bisettrice di un triangolo ABC, la retta r passante per il segmento BC tale che gli angoli aventi lati r-AB e r-AC siano uguali.

Definizione 2.25. Chiamiamo *incentro* di un triangolo ABC, di solito denotato con I, il centro della circonferenza tangente a tutti e tre i lati del triangolo.

Su questa configurazione c'è davvero tanto da dire, noi ci limiteremo a esporre alcuni fatti essenziali:

Lemma 2.26

Preso un angolo generico e la sua retta bisettrice r, i punti appartenenti ad r sono tutti e soli i punti equidistanti dai due lati dell'angolo (nel gergo si dice che la retta r è il luogo dei punti equidistanti dalle due rette che sono i lati del triangolo).

Non è difficile vedere come il prossimo lemma sia una diretta conseguenza del precedente:

Corollario 2.27

Dato un triangolo ABC, le tre bisettrici concorrono sempre in un punto, e questo punto coincide con l'incentro del triangolo.

Infine ecco un importante teorema sulle bisettrici:

Teorema 2.28 (Teorema della bisettrice)

Se in un triangolo ABC tracciamo la bisettrice passante per A, e denotiamo con D il punto in cui questa interseca il segmento BC, allora vale sempre la seguente relazione:

$$\frac{AB}{AC} = \frac{BD}{DC}$$

Questo ovviamente funziona anche con la B-bisettrice e con la C-bisettrice. Inoltre notiamo che il risultato vale anche se la retta passa per A e biseca l'angolo esterno del triangolo con vertice in A (lo stesso si può dire di B e C).

§2.3.4 Ortocentro

§2.4 Lunghezze e Aree

Segue uno spam di fatti di teoria su lunghezze e aree:

Teorema 2.29 (Pitagora)

Dato un triangolo rettangolo di lati a, b e c dove c è l'ipotenusa, vale la seguente relazione:

$$a^2 + b^2 = c^2$$

Teorema 2.30 (Euclide)

Dato un triangolo rettangolo di lati a, b e c dove c è l'ipotenusa, se h è l'altezza relativa all'ipotenusa e a' e b' sono rispettivamente la proiezione di a su c e la proiezione di b su c, sussistono le seguenti relazioni:

$$h^2 = a'b'$$

$$a^2 = a'c$$

$$b^2 = b'c$$

Teorema 2.31 (Erone)

Dato un triangolo qualsiasi di lati a, b e c, se p è il suo semiperimetro (cioè, $p = \frac{a+b+c}{2}$) e A la sua area, sussiste la seguente relazione:

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

Teorema 2.32 (Circumraggio)

Dato un triangolo qualsiasi di lati a, b e c, se R è il raggio della sua circonferenza circoscritta (la circonferenza passante per tutti i suoi tre vertici) e A la sua area, sussiste sempre la seguente relazione:

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

Teorema 2.33 (Inraggio)

Dato un triangolo qualsiasi di semiperimetro p e area A, se r è il raggio della sua circonferenza inscritta (la circonferenza tangente a tutti i suoi lati), sussiste la seguente relazione:

$$r = \frac{A}{p}$$

Teorema 2.34 (Viviani)

Preso un triangolo equilatero ABC, e preso un punto P interno ad esso, la somma delle distanze tra il punto P e i lati è uguale all'altezza del triangolo.

Teorema 2.35 (Triangolo da 45-45)

In un triangolo rettangolo i cui angoli misurano rispettivamente 90, 45 e 45 gradi, il rapporto tra l'ipotenusa e uno dei due cateti (ipotenusa/cateto) vale sempre $\sqrt{2}$.

Teorema 2.36 (Triangolo da 30-60)

In un triangolo i cui angoli misurano rispettivamente 30, 60 e 90 gradi, sussistono le seguenti relazioni:

$$\frac{\text{Ipotenusa}}{\text{Cateto Minore}} = 2$$

$$\frac{\text{Ipotenusa}}{\text{Cateto Maggiore}} = \frac{2}{\sqrt{3}}$$

$$\frac{\text{Cateto Maggiore}}{\text{Cateto Minore}} = \sqrt{3}$$

Definizione 2.37 (Similitudine)**.** Diciamo simili e scriviamo $ABC \sim A'B'C'$ due triangoli ABC e $A'B'C'$ che hanno tutti gli angoli uguali a due a due.

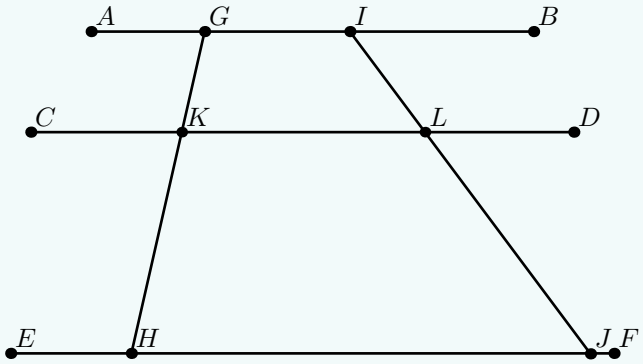
Teorema 2.38 (Criteri di Similitudine)

I seguenti tre fatti sono equivalenti tra loro, e sono equivalenti a $ABC \sim A'B'C'$:

- Gli angoli di ABC e $A'B'C'$ sono uguali a due a due.
- I triangoli hanno due lati in proporzione (il rapporto tra i due lati in questione di ABC è uguale a quello dei due lati di $A'B'C'$) e l'angolo compreso uguale tra loro.
- I triangoli hanno tutti e tre i lati in proporzione (cioè se a, b, c sono i lati di ABC e a', b', c' i lati di $A'B'C'$, abbiamo che esiste un certo numero reale k tale che $a = ka'$, $b = kb'$ e $c = kc'$.

Teorema 2.39 (Talete)

Nella figura sotto se le due rette AB ed EF sono parallele, sussiste la seguente doppia implicazione logica: CD è parallelo ad AB e ad EF se e solo se $\frac{GK}{KH} = \frac{IL}{LJ}$.



Teorema 2.40 (Tolomeo)

Se $ABCD$ è un quadrilatero non intrecciato e AB, BC, CD e DA sono i suoi lati, allora $ABCD$ *cyc* se e solo se la seguente relazione sussiste tra i lati e le diagonali AC e BD:

$$AB \cdot CD + BC \cdot DA = AC \cdot BD$$

§3 Algebra

§3.1 Polinomi

Che cos'è un polinomio? Definiamo prima la nozione di monomio:

Definizione 3.1. Un monomio è un'espressione letterale, come ad esempio, $4x^2yz$, formata dal prodotto di una o più variabili distinte, ciascuna elevata ad una potenza naturale (**NB** naturale significa possibilmente 0), moltiplicate per un coefficiente numerico.

Ok, una volta capito questo possiamo definire la nozione di polinomio in una variabile. In questa sezione ci occuperemo solo di quest'ultimo tipo di polinomi.

Definizione 3.2. Diciamo P polinomio nella variabile x, e scriviamo $P(x)$, una somma di uno o più monomi nella cui parte letterale compare solo la variabile x elevata ad una potenza naturale. Un esempio di ciò è:

$$P(x) = 3x^4 + 2x + 1$$

In generale, un polinomio in una variabile generico si scrive come:

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

dove gli a_i sono coefficienti, e X è la variabile.

Definizione 3.3. Definiamo grado di un polinomio $P(x)$ e scriviamo $\deg(P(x))$ l'esponente massimo con cui compare la x nella scrittura di $P(x)$. Per esempio:

$$\deg(3x^5 + 2x^2) = 5$$
$$\deg(98x^{420} + 42x^5 + 69x^2 + 104) = 420$$

Teorema 3.4

Per operazioni tra polinomi $P(x)$ e $Q(x)$ di grado rispettivamente $p > 0$ e $q > 0$ valgono le seguenti:

$$\deg(P(x) \pm Q(x)) \leq \max(p, q)$$
$$\deg(P(x)Q(x)) = p + q$$

Definizione 3.5. Si dice che valutiamo il polinomio $P(x)$ nel numero a, e scriviamo $P(a)$, quando sostituiamo nell'espressione di $P(x)$ ad ogni x il numero a e svolgiamo le rispettive somme e prodotti. Per esempio, se $P(x) = x^3 - 2x - 4$:

$$P(1) = 1^3 - 2 \cdot 1 - 4 = -5$$
$$P(2) = 2^3 - 2 \cdot 2 - 4 = 0$$
$$P(3) = 3^3 - 2 \cdot 3 - 4 = 17$$

Definizione 3.6. Definiamo *zero* o *radice* di un polinomio $P(x)$ un numero a tale che $P(a) = 0$. Per esempio 2 è radice di $P(x) = x^3 - 2x - 4$ perchè $P(2) = 0$.

Definizione 3.7. Chiamiamo coefficiente direttore di un polinomio il coefficiente del monomio di grado massimo che forma il polinomio, diciamo che un polinomio è monico se il suo coefficiente direttore è 1. Chiamiamo inoltre termine noto di un polinomio il coefficiente del termine d grado 0 del polinomio (possibilmente il termine noto può essere 0 se non vi è monomio di grado 0 nella scrittura del polinomio).

Enunciamo ora un importantissimo teorema che viene di solito trattato il primo anno:

Teorema 3.8 (Divisione tra polinomi)

Dati due Polinomi $A(x)$ e $B(x)$ esistono sempre due polinomi $Q(x)$ e $R(x)$ tali che:

$$A(x) = Q(x)B(x) + R(x)$$
$$0 \leq \deg(R(x)) < \deg(B(x))$$

Definizione 3.9. Diciamo che $B(x)$ divide $A(x)$, e scriviamo $B(x) \mid A(x)$ se $R(x) = 0$.

Teorema 3.10 (Ruffini)

se $P(x)$ è un polinomio, e a un suo zero, allora $x - a$ divide sempre $P(x)$ cioè esiste un polinomio $Q(x)$ tale che:

$$P(x) = (x - a)Q(x)$$

Inoltre è vero anche il contrario, cioè se $x - a$ divide $P(x)$ allora $P(a) = 0$.

Da questo teorema discendono risultati altrettanto enormi e famosi, ne elenchiamo alcuni importanti:

Teorema 3.11 (Teorema Fondamentale dell'Algebra)

Un polinomio di grado n ha al più n radici reali (numeri reali che sono sue radici), e esattamente n radici complesse (radici che sono numeri complessi).

Teorema 3.12 (Principio di uguaglianza dei polinomi)

Due polinomi si dicono uguali quando si possono scrivere allo stesso modo tramite manipolazioni algebriche, o quando sono uguali se valutati in ogni valore. Inoltre si dimostra che due polinomi di grado n sono uguali se sono uguali quando valutati in almeno $n + 1$ valori.

Teorema 3.13 (Fattorizzazione unica)

Dato un polinomio $P(x)$ di grado n, avente radici $\lambda_1, \lambda_2, \ldots \lambda_k$ con $k \leq n$ possiamo "fattorizzarlo" cioè scriverlo unicamente come prodotto di polinomi, nel seguente modo:

$$P(x) = a(x - \lambda_1)(x - \lambda_2)\ldots(x - \lambda_k)Q(x)$$

Dove a è il coefficiente direttore del polinomio, $Q(x)$ è un polinomio di grado $n - k$ privo di radici reali, che è $Q(x) = 1$ se e solo se $k = n$. Inoltre si dimostra che questa fattorizzazione è l'unica che minimizza i gradi di ciascun polinomio coinvolto nel prodotto.

Da questo teorema discendono le cosiddette formule di Vieté e quelle di Newton-Girard, che sono cruciali per risolvere i problemi di algebra delle olimpiadi di matematica:

Teorema 3.14 (Viète)

Facendo riferimento alla notazione della definizione 3.2, e chiamando x_1, x_2, …, x_n tutte le radici complesse del polinomio P di grado n:

$$\sum_{1\leq i_1<i_2<\cdots<i_k\leq n} x_{i_1}x_{i_2}\cdots x_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}$$

Ovvero, la somma di tutti i possibili prodotti ottenibili prendendo k radici del polinomio $P(x)$ prese con le rispettive molteplicità è uguale a $-\frac{a_{n-k}}{a_n}$ se k è dispari, e $\frac{a_{n-k}}{a_n}$ se k è pari.

Teorema 3.15 (Newton-Girard)

Usando la stessa notazione di sopra, se definiamo S_a, con $a \in \mathbb{N}$, la somma delle radici elevate alla a del polinomio, ovvero:

$$S_a = x_1^a + x_2^a + x_3^a + \cdots + x_n^a$$

Abbiamo la seguente elegante identità:

$$0 = a_0 k + a_1 S_1 + a_2 S_2 + a_3 S_3 + \cdots + a_k S_k$$

Per ogni $1 \leq k \leq n$. Questo permette più o meno agevolmente di calcolare *ricorsivamente* tutte le somme S_k in funzione dei coefficienti del polinomio.
Inoltre possiamo generalizzare questo con le seguente formula:

$$0 = a_0 S_k + a_1 S_{k+1} + a_2 S_{k+2} + \cdots + a_n S_{k+n}$$

Per ogni $k \in \mathbb{Z}$. Questo è ulteriormente generalizzabile a $k \in \mathbb{R}$ o addirittura $k \in \mathbb{C}$, purchè imponiamo delle ragionevoli condizioni sul segno delle radici, o accettiamo che gli S_k possano essere complessi.

Infine vediamo alcuni fatti di teoria utilissimi, slegati dal resto:

Definizione 3.16. Diciamo che un polinomio $P(x)$ ha come insieme di coefficienti A e scriviamo $P \in A[x]$ se i coefficienti dei termini che lo formano appartengono tutti ad A.

Teorema 3.17

se $P \in \mathbb{Z}[x]$ allora per ogni $a, b \in \mathbb{Z}$ abbiamo:

$$a - b \mid P(a) - P(b)$$

Teorema 3.18 (RRT/Teorema delle Radici Razionali)

Preso un polinomio $A \in \mathbb{Z}[x]$ le sue radici che appartengono all'insieme dei numeri razionali sono della forma $\pm\frac{p}{q}$ dove p è un divisore del termine noto, e q un divisore del coefficiente direttore.

§3.2 Identità note

Segue uno spam di identità che potete dare per note:

Teorema 3.19 (Binomio di Newton)

La segente identità è vera per ogni $a, b \in \mathbb{R}$ e per ogni $n \in \mathbb{N}$:

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \binom{n}{3}a^{n-3}b^3 \cdots + \binom{n}{n-1}ab^{n-1} + b^n$$

In particolare si ricordano i casi specifici per $n = 2$ e per $n = 3$:

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

(Se non si ricordasse il significato di quelle espressioni in parentesi, si rimanda alla Definizione 4.11)

Teorema 3.20

La seguente identità vale per ogni $a, b \in \mathbb{R}$ e per ogni $n \in \mathbb{N}$:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1})$$

In particolare si ricorda il caso specifico per $n = 1$:

$$a^2 - b^2 = (a-b)(a+b)$$

Teorema 3.21

La seguente identità vale per ogni $a, b \in \mathbb{R}$ e per ogni $n \in \mathbb{N}$ dispari:

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots - ab^{n-2} + b^{n-1})$$

Teorema 3.22 (Gauss)

La segente identità è vera per ogni $n \in \mathbb{N}$:

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

Teorema 3.23 (Somma dei quadrati)

Per ogni $n \in \mathbb{N}$ vale la seguente identità:

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Teorema 3.24 (Nicomaco)

La seguente identità è vera per ogni $n \in \mathbb{N}$:

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

Teorema 3.25 (Serie Geometrica)

La seguente identità è vera per ogni $n \in \mathbb{N}$ e per ogni $x \neq 1 \in \mathbb{R}$:

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

Teorema 3.26 (Formula Quadratica)

l'equazione nell'incognita x e con parametri $a \neq 0, b, c \in \mathbb{R}$

$$ax^2 + bx + c = 0$$

detto k il numero di soluzioni reali, e definito $\Delta := b^2 - 4ac$, abbiamo:

$$k = \begin{cases} 0 & \text{se} \quad \Delta < 0 \\ 1 & \text{se} \quad \Delta = 0 \\ 2 & \text{se} \quad \Delta > 0 \end{cases}$$

e le soluzioni reali, se esistono, sono date dalla seguente formula:

$$x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a}$$

§3.3 Ricorsione

Questa sezione tratta tecniche risolutive che non sono esclusive dell'algebra, e che anzi trovano applicazione principalmente in informatica, o nella cugina combinatoria. La ricorsione è una tecnica di risoluzione dei problemi che consiste nell'identificare una versione identica del problema che stiamo cercando di risolvere all'interno dello stesso. Come per tutte le tecniche risolutive, un esempio vale più di mille parole.

Esempio 3.27

Supponiamo di voler trovare il valore della seguente onirica espressione

$$\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\dots}}}}$$

che prosegue **all'infinito**. Come possiamo fare? Beh, chiamiamo questo numero x per comodità. Notiamo una proprietà molto interessante di x, e cioè che:

$$x = \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\dots}}}} = \sqrt{1+x}$$

Incredibile vero? x è uguale alla radice di uno più se stesso! Cioè il problema che volevamo risolvere (trovare il valore di x) contiene una versione di se stesso al suo interno.
Quindi come troviamo x? Beh x è un numero positivo molto particolare, infatti soddisfa la seguente equazione:

$$x = \sqrt{x+1} \iff x^2 = x+1 \iff x^2 - x - 1 = 0$$

Questa è un'equzione di secondo grado molto famosa, e possiamo risolverla con 3.26. La soluzione (tenendo conto che x è positivo) risulta essere:

$$\frac{1+\sqrt{5}}{2}$$

Che è il famoso *rapporto aureo* e si indica di solito con il simbolo φ (la lettera greca Phi, che si legge "fi").

Esempio 3.28

Supponiamo di voler trovare il valore della seconda seguente onirica espressione:

$$\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\dots}}}}$$

che come prima prosegue **all'infinito**. Come prima chiamiamo questo numero x. Possiamo identificare di nuovo x dentro alla definizione di x? Certo che sì. x è infatti definito nel seguente modo:

$$x = \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\dots}}}} = \frac{1}{1+x}$$

Di nuovo x compare nella sua stessa definizione! Come prima risolviamo l'equazione di secondo grado che troviamo in questo modo:

$$x = \frac{1}{1+x} \iff x(x+1) = 1 \iff x^2 + x = 1 \iff x^2 + x - 1 = 0$$

Che svolgendo i calcoli con 3.26 scopriamo avere soluzioni $\varphi - 1$ e $-\varphi$, quindi dato che x deve essere positivo abbiamo che $x = \varphi - 1$.

§4 Combinatoria

§4.1 Conteggi

Molte volte nella vita vi capiterà di imbattervi in un insieme di elementi, e di chiedervi: "Quanti sono?"
La combinatoria (almeno nella sua accezione meno olimpica) è la branca della matematica dedita a rispondere a questa domanda, e in questa sezione vedremo la teoria fondamentale della materia.

§4.1.1 Somma e Prodotto

Definizione 4.1. Se A è un insieme, denotiamo con $|A|$ il numero di elementi contenuti nell'insieme A e lo chiamiamo *cardinalità*.

Se dobbiamo scegliere due elementi rispettivamente uno da un insieme A e l'altro da un'insieme B, diamo le seguenti definizioni:

Definizione 4.2. Due scelte come descritte sopra si dicono indipendenti
quando $A \cap B = \emptyset$ (formalmente l'insieme di tutti gli esiti di queste scelte sarebbe il prodotto cartesiano tra i due insiemi A e B, denotato con $A \times B$, se conoscete già questa operazione e ci siete abituati, bene; altrimenti un'intuizione come descritta prima è più che sufficiente).

Valgono i seguenti importanti teoremi:

Teorema 4.3 (Prodotto Logico)
Il numero possibile di scelte indipendeti di due elementi, uno dall'insieme A, e l'altro dall'insieme B, di cardinalità a e b è $a \cdot b$ (riprendendo quanto è stato detto prima, questo risultato formalmente sarebbe l'identità per gli insiemi finiti A e B: $|A \times B| = |A| \cdot |B|$).

Ricordiamo il seguente fatto di teoria degli insiemi[2]:

Teorema 4.4 (Somma Logica)
Se abbiamo gli insiemi A, B disgiunti (cioè con intersezione nulla, ovvero $A \cap B = \emptyset$) e dobbiamo scegliere un singolo elemento appartenente a uno dei due insiemi, il numero di possibilità che abbiamo è:

$$|A \cup B| = |A| + |B|$$

Tutte le formule di combinatoria si possono essenzialmente ridurre ad un'applicazione iterata di queste due operazioni, che è bene sapere.
Un a terza importante operazione è quella che ci permette di avere a che fare (anche se in modo relativamente caotico) con le intersezioni:

[2] finiti

Lemma 4.5 (Principio di Inclusione-Esclusione)

Dati due insiemi A e B, la cardinalità della loro unione vale:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Questo fatto si può generalizzare, ad una espressione complicata quando gli insiemi considerati non sono due ma n. Sinteticamente per n insiemi A_1, A_2, A_3, ..., A_n vale:

$$\begin{aligned}|A_1 \cup A_2 \cup A_3 \cup A_4 \dots A_n| =& |A_1| + |A_2| + |A_3| + \dots + |A_n| \\ &- (|A_1 \cap A_2| + |A_1 \cap A_3| \dots + |A_n \cap A_{n-1}|) \\ &+ |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| \dots\end{aligned}$$

Cioè, l'unione è uguale alla somma delle cardinalità degli insiemi, meno le cardinalità di tutte le intersezioni tra due insiemi distinti, più le cardinalità delle intersezioni fra tre insiemi distinti, meno le cardinalità delle intersezioni fra quattro insiemi distinti...e così via fino a che non si considerano le intersezioni fra n insiemi distinti.

Come si intuisce da sopra, lavorare con le intersezioni *fa schifo*, quindi cercate sempre di trovare strade più furbe di applicare alla lettera il principio sopra quando non potete ricondurvi al caso con soli due insiemi.

§4.1.2 Anagrammi

Definizione 4.6. Chiamiamo *anagramma* di una parola, una parola formata dallo stesso numero di lettere e dello stesso tipo, disposte in un certo ordine, possibilmente diverso da quello della parola di partenza (**ATTENZIONE**: qui per anagrammi intendiamo anche parole prive di significato).

Definizione 4.7. Dato $n \in \mathbb{N}_0$ definiamo il suo *fattoriale* e scriviamo $n!$ come:

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

Precisiamo che questa definizione non vale per $n = 0$, per cui vale invece $0! = 1$.

Chiediamoci allora: "Quanti sono gli anagrammi di una certa parola data? Approfondiamo la questione in questa sottosezione.

Teorema 4.8 (Anagrammi senza ripetizioni)

Una parola formata da n lettere distinte ha esattamente $n!$ anagrammi.

Teorema 4.9 (Anagrammi con una Ripetizione)

Una parola formata da n lettere distinte e da k lettere uguali ha esattamente

$$\frac{(n+k)!}{k!}$$

anagrammi.

E da qui è facile generalizzare per una parola arbitraria:

Teorema 4.10 (Anagrammi con Ripezioni)

Se una parola formata da n lettere ha k insiemi di lettere uguali, ciascuno rispettivamente di cardinalità a_1, a_2, $\ldots a_k$, il numero dei suoi anagrammi è esattamente:

$$\frac{n!}{a_1!a_2!a_3!\ldots a_k!}$$

Gli anagrammi sono degli strumenti sorprendentemente versatili, che trovano applicazioni inusuali ad una enorme moltitudine di problemi olimpici. Per esempio, tra i più famosi abbiamo il numero di percorsi di lunghezza $n+m$ in una tabella $m \times n$ che partono da un angolo e arrivano a quello opposto, che possono essere visti come gli anagrammi della parola DDD…DSSS…S formata da m lettere D e n lettere S, ognuna di queste rappresenta una possibile mossa verso destra (D) o verso su (S) nella tabella.
In generale quando vi rendete conto che il problema che state cercando di risolvere può essere messo in relazione con gli anagrammi di qualche parola costruita *ad-hoc*, dovreste sempre essere molto felici di approfondire quella strada e utilizzare le formule sopra per chiudere il problema.

§4.1.3 Binomiali

Un particolare tipo di anagramma è quello che ci permette di calcolare il numero di modi in cui possiamo scegliere k elementi distinti da un insieme di n, a meno dell'ordine.

Definizione 4.11. Se $n, k \in \mathbb{N}$ e $n \geq k$ chiamiamo coefficiente binomiale una scrittura come quella che segue, e la definiamo in questo modo:

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

La scrittura a sinistra dell'uguaglianza si legge spesso come "n scelto k", oppure come "n choose k" oppure come "n su k". Inoltre se $n < k$ definiamo il coefficiente binomiale come:

$$\binom{n}{k} := 0$$

Dunque vale il seguente teorema

Lemma 4.12

Il numero di modi per scegliere k elementi da un insieme di cardinalità n è precisamente $\binom{n}{k}$.

Questo si può dimostrare anagrammando la parola 0000…00111…11 formata da n caratteri, di cui k caratteri 1. I coefficienti binomiali sono certo utili per risolvere problemi di combinatoria riguardanti conteggi, ma sono anche fondamentali per risolvere problemi di algebra, tramite le seguenti identità, che potete dare per note:

Lemma 4.13

La seguente identità vale per ogni $n > k \in \mathbb{N}$:

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

Lemma 4.14

La seguente identità vale per ogni $n \in \mathbb{N}$:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

Si noti che questa identità puo seguire da 3.19.

Lemma 4.15

La seguente identità vale per ogni $n \geq k \in \mathbb{N}$:

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

In particolare ricordiamo le seguenti identità per valori notevoli di k:

$$\binom{n}{0} = \binom{n}{n} = 1$$
$$\binom{n}{1} = \binom{n}{n-1} = n$$

Lemma 4.16 (Mazza da Hockey)

Dati $n, k \in \mathbb{N}$ vale sempre la seguente identità:

$$\binom{1}{k} + \binom{2}{k} + \binom{3}{k} + \cdots + \binom{n-1}{k} + \binom{n}{k} = \binom{n+1}{k+1}$$

Lemma 4.17 (Vandermonde)

La seguente identità vale per ogni m, n, $a \in \mathbb{N}$:

$$\binom{m+n}{a} = \binom{m}{0}\binom{n}{a} + \binom{m}{1}\binom{n}{a-1} + \binom{m}{2}\binom{n}{a-2} + \cdots + \binom{m}{a}\binom{n}{0}$$

§4.2 Tecniche Dimostrative

Come disse un saggio[3], la C che di solito si trova ad indicare la quarta materia della matematica olimpica sta per "combinatoria", ma anche per "cose a caso".
Questo significa che di solito vanno sotto la definizione di combinatoria (a livello olimpico) anche molti problemi dimostrativi che vengono percepiti come "puro ragionamento" oppure come teoria dei giochi base. L'obbiettivo di questa sezione è introdurre le principali strategie risolutive di problemi di questo tipo, tenendo presente che l'unico modo per capirle e saperle applicare in contesti originali è fare molta pratica risolvendo problemi (questo è vero in generale per la matematica olimpica, specialmente per i problemi dimostrativi, ancora di più per i problemi dimostrativi di combinatoria).

§4.2.1 Induzione

La prima importante strategia per risolvere problemi dimostrativi, sia di combinatoria che non, è l'induzione. Come funziona l'induzione? a livello formale il principio di induzione è un assioma, ed è formulato così:

Proposizione 4.18 (Induzione)

Sia P una proposizione[a] il cui valore di verità (cioè il fatto che sia vera o falsa) dipende dalla variabile $n \in \mathbb{N}$[b], scriviamo $P(n)$ per questo particolare tipo di proposizioni. Se $P(0)$ è vera e se il fatto che $P(k)$ sia vera implica il fatto che $P(k+1)$ sia a sua volta vera, abbiamo che $P(n)$ è vera per ogni $n \in \mathbb{N}$, in simboli per ogni $n \in \mathbb{N}$ vale:

$$P(0) \wedge (P(k) \implies P(k+1)) \qquad \implies \qquad P(n)$$

[a] Una affermazione per la quale si può dire oggettivamente se è vera o falsa, per esempio "due è uguale a due" oppure "In questo momento sta piovendo".
[b] Nel gergo della logica matematica questo viene detto "Enunciato Aperto", perché non gli si può assegnare un valore di verità prima di aver assegnato il valore della variabile n e rimane quindi "aperto".

Molto bene. Cosa diamine significa?
Possiamo vederlo intuitivamente come un modo per costruire infinite dimostrazioni del fatto che la proposizione P sia vera. Facciamo un esempio dimostrando il teorema 3.22.

Dimostrazione. Vogliamo dimostrare che il seguente fatto vale per ogni $n \in \mathbb{N}$:

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

Per prima cosa verifichiamo che $P(0)$ sia vera, cioè che sostituendo a n il valore 0 l'espressione risultante sia vera:

$$0 = 1 + 2 + 3 + \cdots + 0 = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} = \frac{0 \cdot (0+1)}{2} = 0$$

Quindi sostituendo a n il numero 0 otteniamo $0 = 0$, che è certamente vera. Dunque abbiamo che $P(0)$ è vera. Ora come facciamo a dimostrare che $P(n)$ è vera per tutti gli altri numeri senza dover fare infinite sostituzioni? Beh, possiamo notare che se la proposizione vale per un certo numero k, allora abbiamo:

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$$

[3] di cui gli autori non ricordano il nome, purtroppo.

Questo è chiaro, è semplicemente il nostro enunciato. Ma cosa succede se sommiamo da entrambi i lati $k+1$? sicuramente il lato sinistro rimane uguale a quello destro, quindi otteniamo di nuovo una proposizione vera, in particolare abbiamo:

$$\begin{aligned} 1+2+3+\cdots+k+(k+1) &= \frac{k(k+1)}{2}+(k+1) \\ &= (k+1)\left(\frac{k}{2}+1\right) \\ &= (k+1)\frac{k+2}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

Che, miracolo, scopriamo essere $P(k+1)$! cioè l'espressione che si trova sostituendo alla n il numero $k+1$ nella nostra espressione di partenza. Abbiamo quindi dimostrato che $P(k+1)$ è vera. Ecco, questo ora è il fulcro del principio di induzione: noi sappiamo che preso un generico numero k, se la tesi è vera per k lo è anche per $k+1$, ma noi sappiamo che $P(0)$ è vera, quindi sicuramente anche $P(1)$ è vera. Ma ora sappiamo che $P(1)$ è vera, quindi (sempre perchè se $P(k)$ è vero allora lo è anche $P(k+1)$) anche $P(2)$ è vera. Per lo stesso motivo $P(3)$ sarà vera, e così anche $P(4)$, $P(5)\ldots$
Insomma, possiamo andare avanti all'infinito, per ogni numero naturale n possiamo verificare che $P(n)$ sia vero in un numero finito di passaggi, ci basta passare da $P(0)$ a $P(1)$ a $P(2)\ldots$fino a $P(n-1)$ e poi finalmente a $P(n)$.
Ecco il principio di induzione serve proprio a formalizzare questo strano passaggio logico, quando troviamo una proposizione che soddisfa la proprietà chiave $P(k) \implies P(k+1)$ e riusciamo a dimostrare che un certo $P(a)$ è vero, allora $P(n)$ sarà vera per ogni $n \in \mathbb{N}$ tale che $n \geq a$. Questo modo di risolvere i problemi è straordinariamente potente, ma per evitare di incorrere in spiacevoli inconvenienti è bene imparare a scrivere bene le dimostrazioni per induzione. Di solito seguono uno schema di questo tipo.

Dobbiamo dimostrare che:

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

Per ogni $n \in \mathbb{N}$.
Procediamo per induzione:

- **Passo base** $P(0)$ è vera perchè sostituendo da ambo i lati 0 otteniamo $0=0$ che è evidentemente vera.
- **Passo induttivo, supponiamo che la tesi valga per un certo** $k \in \mathbb{N}$ allora abbiamo:

$$1+2+3+\cdots+k = \frac{k(k+1)}{2}$$

$$\begin{aligned} 1+2+3+\cdots+k+(k+1) &= \frac{k(k+1)}{2}+(k+1) \\ &= (k+1)\left(\frac{k}{2}+1\right) \\ &= (k+1)\frac{k+2}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

quindi la tesi vale anche per $k+1$.

Quindi **per induzione** abbiamo dimostrato la tesi. □

Come già detto, questa tecnica è cruciale per un incredibile numero di problemi di combinatoria, di teoria dei numeri e di algebra (anche se non molti di geometria). In generale le parole evidenziate in grassetto nella dimostrazione sopra sono quelle che non dovrebbero mai mancare in una vostra dimostrazione per induzione, quindi cercate di seguire quello schema, almeno finchè non vi sarete ben abituati. Se si vuole fare esercizio, dimostrare i teoremi 3.23, 3.24 e 3.25 è un ottimo modo per iniziare.
Esiste una formulazione alternativa e più forte del principio di induzione, il ragionamento che c'è dietro è esattamente lo stesso e quindi non ci ripeteremo.

Proposizione 4.19 (Induzione estesa/Induzione forte)

Dato un enunciato aperto $P(n)$ con $n \in \mathbb{N}$, se abbiamo che $P(n)$ vera per ogni $n \leq k$ implica $P(k+1)$ vera, e abbiamo che $P(0)$, $P(1)$, $P(2)\ldots P(k)$ sono veri, allora $P(n)$ è vera per ogni $n \in \mathbb{N}$.

Con l'induzione estesa il passo induttivo diventa:
"supponiamo che la tesi valga per ogni $k \leq n\ldots$ allora la tesi vale per $k+1$". Fate solo attenzione a verificare la seconda condizione, se per dimostrare che $P(k)$ è vero avete bisogno che $P(k-1)$ e $P(k-2)$ siano veri, il passo base consiste nel dimostrare che sia $P(0)$ sia $P(1)$ (**!!!**) sono vere.

§4.2.2 Double counting

"Double counting", come il nome suggerisce, è una tecnica che consiste nel contare in due modi una stessa quantità. I vantaggi di questo approccio sono evidenti nei seguenti esempi.

Esempio 4.20

Supponiamo di voler trovare una dimostrazione alternativa al risultato visto nel capitolo precedente, che affermava che per qualunque $n \in \mathbb{N}$:

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

1	2	3	4	…	$n-1$	n
n	$n-1$	$n-2$	$n-3$	…	2	1

Notiamo che abbiamo due modi per calcolare la somma delle celle della tabella sopra, il primo è sommare riga per riga, e il secondo colonna per colonna. Il punto del double counting è che l'espressione che troviamo in un caso **deve** essere uguale a quella che troviamo nell'altro caso, perchè **stiamo contando la stessa quantità**. In questo caso la somma di una riga risulta essere:

$$1+2+3+4+\cdots+n$$

Quindi la somma delle righe è:

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

Vogliamo ora trovare la somma colonna per colonna. L'osservazione chiave è che, sommando a coppie il primo numero con l'ultimo, il secondo con il penultimo, e così via, la

somma sembrerebbe rimanere costante ed uguale a $n+1$. Ciò è evidente se si nota che nella i-esima colonna la somma trovata è data da:

$$(n+1-i)+i=n+1$$

Quindi la somma totale è $n+1$ moltiplicata per n, che è il numero delle colonne. Da ciò la seguente uguaglianza:

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

Il double counting di solito trova più facilmente applicazione nella dimostrazione di identità combinatoriche, per esempio se vogliamo dimostrare la 4.15 con un double counting possiamo procedere in questo modo:

Esempio 4.21

Vogliamo dimostrare che

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

per ogni $n \geq k \in \mathbb{N}$. Per fare ciò consideriamo un insieme A di n elementi e supponiamo di volerne scegliere k da questo. per il lemma 4.12 ci sono due modi per farlo, il primo è scegliere direttamente i k elementi, e questo lo posso fare in

$$\binom{n}{k}$$

modi. Il secondo è scegliere prima gli $n-k$ elementi che **non** vogliamo scegliere, e questo determinerà univocamente quali saranno gli elementi scelti. In quanti modi lo posso fare? Beh, sto scegliendo $n-k$ elementi da un insieme di n, quindi abbiamo

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

modi per farlo. Abbiamo contato la stessa quantità in due modi, quindi queste due espressioni devono essere uguali, da qui la tesi:

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

Quindi di solito per dimostrare identità con double counting dobbiamo "interpretare" ciascun lato dell'identità (nell'esempio prima, un lato corrisponde a scegliere k elementi, e l'altro a scegliere gli $n-k$ elementi da scartare) dal punto di vista combinatorico, per poi concludere invocando il double counting (bisogna sempre scrivere ciò che si sta facendo). Se si volesse fare esercizio su questo argomento, dimostrare i lemmi 4.13 e 4.14 è un ottimo modo per cominciare.

§4.2.3 Invarianti

"Invariante" è un termine che presenta una definizione molto vaga. Il modo più semplice per spiegarlo è definirlo come una quantità che non varia, oppure che varia ma in maniera controllata; ma il modo più semplice per capirlo è attraverso degli esempi.

Esempio 4.22

Suppongo di avere un numero n scritto su una lavagna. Ad ogni mossa, posso permutare[a] le cifre della sua rappresentazione decimale. Allora la somma delle cifre del numero dopo ogni mossa non varia, dunque è un'**invariante**.

[a] permutazione è un altro termine per indicare un anagramma (teoremi 4.8, 4.9 e 4.10), quindi permutare qualcosa significa scriverne un particolare anagramma.

Esempio 4.23

Suppongo di avere il numero 2 scritto su una lavagna. Ad ogni mossa, posso scegliere se sommare 5 o 3 al numero scritto, e sostituire il numero sulla lavagna con il valore, che chiamo n, della somma. Noto che così facendo, la parità di n cambia ad ogni mossa; in particolare, essendo che il numero di partenza era pari, n sarà pari dopo che effettuo un numero pari di mosse, e dispari dopo un numero dispari di mosse. Quindi questa parità varia in modo controllato, dunque è un'**invariante**.

§4.2.4 Pigeonhole

Il pigeonhole, o principio dei cassetti, formalizza un concetto molto semplice e logico:

Proposizione 4.24 (Pigeonhole)

Se ho n cassetti, e $n+1$ oggetti che voglio disporre all'interno di questi, allora esisterà almeno un cassetto con più di un oggetto al suo interno.