Appunti di Matematica Discreta
Corso di studi in Informatica
a.a. 2018-19

Materiale proveniente da:

- "Appunti provvisori del corso di Matematica Discreta" di Alessandro Berarducci e Giovanni Gaiffi.
- "Appunti delle lezioni del corso di Aritmetica" di Giovanni Gaiffi
- Il capitolo sui polinomi è tratto da dispense di Giovanni Gaiffi e Pietro Di Martino

Collage e aggiustamenti a cura di Alessandro Berarducci che ringrazia Gaiffi e Di Martino per aver messo a disposizione il materiale ed è responsabile per errori e sviste.

Indice

CAPITOLO 1

Proposizioni e Connettivi

1. Considerazioni introduttive

1.1. Uguaglianza. Le dimostrazioni più semplici che uno studente incontra nel corso della sua carriera scolastica sono quelle "per sostituzione", ovvero quelle che si ottengono in base alla seguente *legge di sostituzione degli uguali*: se $a = b$, allora a e b verificano le stesse proprietà, e pertanto possiamo sostituire a con b in qualunque contesto $P(a)$ in cui si faccia riferimento ad a ottenendo $P(b)$. Ad esempio sapendo che $12 - 10 = 2$ posso dedurre che $8 \cdot (12 - 10) = 8 \cdot 2$. [1]

Possiamo rappresentare in forma grafica la regola di sostituzione nel modo seguente:

$$\frac{a = b,\ P(a)}{P(b)}$$

1.2. Ipotesi e tesi. Se le dimostrazioni per sostituzione non pongono in genere grossi problemi, maggiori difficoltà vengono invece incontrate nello studio delle disuguaglianze. In genere più che di difficoltà di calcolo (come potrebbe esserlo la semplificazione di una espressione complessa), si tratta di difficoltà di tipo logico, come ad esempio lo scambiare l'ipotesi con la tesi, ovvero tra *ciò che assumiamo come vero* (l'**ipotesi**) con *ciò che vogliamo dimostrare essere vero* (la **tesi**). Un punto che spesso non viene compreso è che quando diciamo che una data tesi *segue* (o è *implicata*) dalla data ipotesi intendiamo dire che affinché la tesi sia vera è *sufficiente* che l'ipotesi sia vera, ma non che è *necessario* che lo sia: ovvero in tutti i casi in cui l'ipotesi è vera lo deve essere anche la tesi, ma la tesi potrebbe essere vera "per i fatti suoi" anche in altri casi, ovvero anche in certi casi in cui l'ipotesi è falsa. Detto in altri termini, affinché la tesi segua dall'ipotesi l'unica cosa importante è che non esista alcun caso in cui l'ipotesi sia vera e la tesi sia falsa (se l'ipotesi è sempre falsa tanto meglio: in questo caso la tesi segue "a vuoto"). Le difficoltà nel comprendere questi concetti si riscontrano soprattutto quando, nel corso di una dimostrazione, vengono introdotte condizioni o ipotesi aggiuntive che ci si riserva di verificare o di "scaricare" prima della fine della dimostrazione.

ESEMPIO 1.1. Sia k un numero intero non negativo e supponiamo che

$$2^k \geq 2k^2 - 10k + 21. \tag{Ipotesi}$$

Ci domandiamo se è possibile dedurne che

$$2^k \geq k^2 - 3k + 12. \tag{Tesi}$$

SOLUZIONE: In questo esempio abbiamo tre quantità:

[1] Nel linguaggio ordinario talvolta si incontrano apparenti violazioni del principio di sostituzione: ad esempio "Pierre crede che $2^{2^5} + 1$ sia primo" non equivale a "Pierre crede che 641×6700417 sia primo", nonostante $2^{2^5} + 1$ sia di fatto uguale a 641×6700417 (ma Pierre potrebbe non saperlo!). Il problema è che con "crede che" introduciamo un contesto in cui non si fa esclusivo riferimento alle entità $2^{2^5} + 1$ e 641×6700417 ma anche al modo in cui vengono presentate.

$$\begin{aligned} A &= 2^k \\ B &= 2k^2 - 10k + 21 \\ C &= k^2 - 3k + 12 \end{aligned}$$

L'ipotesi dice che $A \geq B$. Quello che vogliamo sapere è se $A \geq C$. Una cosa naturale da fare è cercare di confrontare B e C. Si tratta di un compito non troppo difficile trattandosi di espressioni di secondo grado. Però cosa dobbiamo cercare di dimostrare? Che $B \geq C$ o che $C \geq B$? Un attimo di riflessione mostra che, ferma restando l'ipotesi principale $A \geq B$, la condizione aggiuntiva $B \geq C$ è *sufficiente* per avere la tesi: se tale condizione fosse verificata componendo le disuguaglianze $A \geq B$ e $B \geq C$ avremmo la tesi $A \geq C$. (Per analogia: se so che il signor A è più alto di B, e che B è più alto di C, posso concludere che A è più alto di C.) Cerchiamo dunque di capire se $B \geq C$, ovvero se

$$2k^2 - 10k + 21 \geq k^2 - 3k + 12.$$

Con facili semplificazioni tale condizione risulta equivalente a

$$k^2 + 9 \geq 7k,$$

che, come si vede anche ad occhio, è vera per tutti gli interi non negativi k maggiori o uguali a 6 ma è falsa per quelli < 6. Cosa possiamo concluderne? Certamente se introduciamo l'ipotesi ulteriore $k \geq 6$ la tesi risulta vera, essendo verificata la disuguaglianza $B \geq C$ che era per l'appunto una condizione sufficiente per la tesi. Tuttavia senza l'ipotesi aggiuntiva incontriamo una difficoltà in quanto per $k < 6$ la condizione $B \geq C$ è falsa. A questo punto è importante non scoraggiarsi e soprattutto non cadete nell'errore di concluderne frettolosamente che senza assumere $k \geq 6$ non possiamo arrivare alla nostra tesi. La $B \geq C$ era infatti *sufficiente* (in congiunzione con l'ipotesi principale $A \geq B$) per avere la tesi, ma *non necessaria*: ovvero la tesi potrebbe essere vera anche in altri casi oltre a quelli che verificano $B \geq C$. (Proseguendo la nostra analogia: se il signor A è più alto di B ma B non è più alto di C, non posso concludere nulla riguardo al fatto se A sia più alto di C a meno di non riuscire a scoprire altre informazioni utili a riguardo.) L'analisi del problema non è dunque terminata: dobbiamo capire cosa succede per $k < 6$, ovvero nei casi ancora non considerati. Valutando le espressioni A e C si vede che anche per $k = 4$ e $k = 5$ la tesi $A \geq C$ è vera. Bene, stiamo sulla buona strada. Tentiamo ora con $k = 0, 1, 2, 3$. Oibò! Per tali valori la tesi è falsa! Dobbiamo dunque concluderne che la tesi non segue dall'ipotesi? Calma. Ancora un attimo di pazienza: i valori $k = 0, 1, 2, 3$ in realtà non ci interessano affatto in quanto, valutando le espressioni A e B, si vede che non rientrano tra quelli che verificano l'ipotesi $A \geq B$ da cui siamo partiti: assumere che l'ipotesi sia vera significa per l'appunto restringere la nostra attenzione solo ai valori di k che la verificano. L'analisi del problema è ora finalmente terminata, e la conclusione è che la tesi segue in effetti dall'ipotesi. □

Notiamo che se non ci fosse stato nessun valore di k che verificava l'ipotesi, anche in quel caso si poteva concludere che la tesi segue ("a vuoto") dall'ipotesi.

Finiamo con un consiglio spassionato agli studenti: quando risolvete un compito in classe che coinvolge le disuguaglianze, cercate di "condire" il vostro elaborato con locuzioni del tipo: "è necessario che", "è sufficiente che", "abbiamo quindi dimostrato che", e altre espressioni consone che illustrano il ragionamento. Se omettete il ragionamento e lasciate solo i calcoli non si capisce nulla. Ad esempio omettendo il ragionamento e lasciando solo i calcoli nell'esempio precedente avrei qualcosa del tipo:

SOLUZIONE:
$2k^2 - 10k + 2 \geq k^2 - 3k + 12$
$k^2 + 9 \geq 7k$
$k \geq 6$??? □

In seguito daremo alcune regole generali e consigli per scrivere dimostrazioni corrette e leggibili. Prima però dobbiamo studiare le leggi che governano il "vero" e il "falso", in quanto uno dei criteri per stabilire la bontà di una dimostrazione è che essa raggiunga il suo scopo, ovvero che garantisca che nei casi in cui l'ipotesi è vera lo sia anche la tesi.[2]

2. Tavole di verità

Chiamiamo **proposizione** ciò a cui in un dato contesto ha senso attribuire, anche se solo in via ipotetica, uno dei valori "vero" o "falso". Ad esempio "$3 > 2$" è una proposizione vera, mentre "$2 > 3$" è una proposizione falsa. L'inciso "anche se solo in via ipotetica" è importante. Nell'esempio 1.1 abbiamo ad un certo punto introdotto l'ipotesi "$k \geq 6$". In quel contesto $k \geq 6$ va quindi considerata una proposizione (dipendente dal parametro k). Chiaramente presa isolatamente e fuori contesto, non avrebbe senso chiedersi se $k \geq 6$ sia vera o falsa: occorrerebbe dire chi è k.

Assumiamo la concezione classica secondo cui una proposizione è o vera o falsa (principio del terzo escluso), ma non può essere sia vera che falsa (principio di non contraddizione).

I **connettivi booleani** sono usati per costruire proposizioni complesse a partire da proposizioni semplici. Nella formalizzazione del linguaggio matematico i connettivi di cui faremo maggiore uso sono indicati con i simboli $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$. La loro traduzione approssimativa in italiano è la seguente:

"$\neg A$" significa "non A" (negazione),
"$A \wedge B$" significa "A e B" (congiunzione),
"$A \vee B$" significa "A o B" (disgiunzione),
"$A \rightarrow B$" significa "se A, allora B" (implicazione),
"$A \leftrightarrow B$" significa "A se e solo se B" (doppia implicazione).

Le lettere A, B sopra usate indicano generiche proposizioni.

I connettivi booleani sono *vero-funzionali* nel senso che il valore di verità di una proposizione composta dipende solo dal valore di verità delle proposizioni semplici che la costituiscono. Questo avviene secondo le seguenti **tavole di verità** che precisano il significato dei connettivi. Per semplicità scriviamo "**1**" per "vero" e "**0**" per "falso". I possibili *valori di verità* che una proposizione può assumere sono dunque **1** e **0**. Iniziamo con la tavola della negazione.

A	$\neg A$
0	**1**
1	**0**

La tavola dice che la proposizione $\neg A$ è vera se A è falsa, ed è invece falsa se A è vera. La negazione inverte il valore di verità. Diamo ora le tavole degli altri connettivi.

[2]Far dipendere la bontà di una dimostrazione da criteri semantici riguardanti il vero e il falso può non piacere a chi ritiene che siano invece le regole di inferenza ad avere la priorità: qui stiamo seguendo un altro punto di vista.

A	B	$A \wedge B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$
0	**0**	**0**	**0**	**1**	**1**
0	**1**	**0**	**1**	**1**	**0**
1	**0**	**0**	**1**	**0**	**0**
1	**1**	**1**	**1**	**1**	**1**

Le prime due colonne indicano i quattro possibili valori di verità di A e B. Le altre colonne indicano i corrispondenti valori degli enunciati composti $A \wedge B$, $A \vee B$, $A \to B$, $A \leftrightarrow B$.

La tavola di verità del connettivo $\wedge$ dice che $A \wedge B$ è vera se e solo se sia A che B sono vere.

La tavola di verità del connettivo $\vee$ dice che $A \vee B$ è vera se almeno uno di A e B è vero, senza escludere la possibilità che entrambi siano veri. Questa modalità di disgiunzione corrisponde al "vel" della lingua latina e viene chiamata *disgiunzione inclusiva*.

Oltre alla disgiunzione inclusiva $A \vee B$ esiste anche una *disgiunzione esclusiva*, corrispondente all' "aut" latino, che indichiamo con il simbolo $\oplus$ ed è definita dalla seguente tavola di verità:

A	B	$A \oplus B$
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**0**

Consideriamo ora il connettivo $\leftrightarrow$. La tavola dice che $A \leftrightarrow B$ è vera se A e B sono entrambe vere o entrambe false. Se ciò capita diremo che A e B si *equivalgono* o che *sono equivalenti*. Scriveremo anche

$$A \equiv B$$

per affermare che A e B sono equivalenti.

Analizziamo infine la tavola dell'implicazione. Abbiamo visto che lo scopo di una dimostrazione è di garantire che le ipotesi implichino la tesi, quindi l'implicazione è in qualche modo il connettivo più importante. Dalla tavola dell'implicazione risulta che $A \to B$ è falsa solo nel caso in cui la premessa A è vera e il conseguente B è falso. In particolare se la premessa A è falsa, l'enunciato $A \to B$ è sempre vero a prescindere da quale sia l'enunciato B: da una premessa falsa segue ogni proposizione.

Esempio 1.2. Supponiamo che il signor Rossi dica: "se vinco alla lotteria vado a fare il giro del mondo." Questo corrisponde alla proposizione $A \to B$ dove $A =$ vinco alla lotteria, $B =$ vado a fare il giro del mondo. A meno di non fare un processo alle intenzioni, c'è un unico caso in cui possiamo affermare che il signor Rossi dice una cosa falsa: quando per l'appunto A è vera e B è falsa, ovvero lui vince alla lotteria, ma ciò nonostante non va a fare il giro del mondo. In tutti gli altri casi, compreso il caso in cui va a fare il giro del mondo pur non avendo vinto, non possiamo dire che abbia mentito. Ciò è in accordo con la tavola dell'implicazione.

Per affermare che A implica B scriveremo anche $A \implies B$ e diremo che "A è una **condizione sufficiente** per B" (nel senso che per poter asserire B è sufficiente che A sia vera) e che "B è una **condizione necessaria** per A" (cioè, affinché A sia vera è necessario che lo sia anche B). Si noti che A e B si equivalgono se valgono entrambe le implicazioni $A \to B$ e $B \to A$, ovvero A è una condizione *necessaria e sufficiente* per B.

Esempio 1.3. Dato un qualsiasi numero reale x, vale l'implicazione

$$x > 2 \to x^2 > 4. \qquad (*)$$

Infatti se il numero x è scelto in modo da verificare la condizione $x > 2$ allora entrambe le proposizioni $x > 2$ ed $x^2 > 4$ risultano vere, e pertanto lo è anche la (*) in base alla tavola del $\to$. Cosa avviene se invece il numero x è scelto in modo da *non* verificare la condizione $x > 2$? La cosa importante da osservare è che anche in quel caso la (*) è vera, in quanto una implicazione con premessa falsa è sempre vera. Stiamo dunque bene attenti a non confondere la verità di una implicazione $A \to B$ con la verità di A o con quella di B. La proposizione $x > 2 \to x^2 > 4$ è *sempre* vera (cioè anche per i valori di x che non verificano $x > 2$) ma la $x^2 > 4$ non è sempre vera: lo è *a condizione che* $x > 2$ (ma non solamente a quella condizione: x potrebbe essere < -2).

Si noti che l'implicazione inversa $x^2 > 4 \to x > 2$ non vale in generale. La $x > 2$ è sufficiente per avere $x^2 > 4$ ma non è necessaria: come già osservato la $x^2 > 4$ è vera anche nei casi in cui $x < -2$.

3. Come si dimostra una implicazione

La tavola dell'implicazione è congegnata in modo tale che dimostrare la validità di $A \to B$ è perfettamente equivalente a dimostrare B sotto l'ipotesi che A sia vera (perché intanto nel caso in cui A è falsa l'implicazione è vera comunque). Le dimostrazioni di un enunciato della forma $A \to B$ iniziano perciò spesso con una frase del tipo "Assumiamo A" (che equivale a dire "mettiamoci, fino a nuovo ordine, in un caso in cui A è vero"), e procedono con il tentativo di verificare B sotto quella ipotesi. Se si riesce ad ottenere B all'interno della "sotto-dimostrazione" in cui vale l'ipotesi A, si può a quel punto "scaricare l'ipotesi A" (cioè uscire dalla sotto-dimostrazione in cui è in vigore A) e concludere $A \to B$ (l'implicazione essendo vera anche se A è falso).

Per maggiore leggibilità può essere conveniente "indentare" le proposizioni della sotto-dimostrazioni rispetto a quelle della dimostrazione "madre". In forma grafica l'introduzione e lo scaricamento di una ipotesi all'interno di una dimostrazione assume dunque la seguente forma, dove abbiamo indicato con D' la sotto-dimostrazione della dimostrazione D.

Passaggi vari della dimostrazione D
Assumiamo p (inizio della sottodimostrazione D')
Passaggi vari
q
Quindi $p \to q$, scaricando l'ipotesi p (ritorno a D).

Ovviamente tutte le proposizioni valide in D possono essere richiamate in D' ove ce ne sia bisogno. L'introduzione di altre ipotesi può dar luogo a sotto-sotto-dimostrazioni a qualunque livello di profondità.

4. Esempi

Il seguente esempio mostra che non sempre le tavole si accordano perfettamente con l'uso che si fa in italiano dei connettivi.

ESEMPIO 1.4. Date due proposizioni A, B, in base alle tavole $A \wedge B$ equivale a $B \wedge A$. Tuttavia questo non sempre concorda con l'uso della congiunzione "e" in italiano. Ad esempio si confronti "ho preso la medicina e mi sono sentito male" con "mi sono sentito male e ho preso la medicina". È presumibile che chi pronuncia queste frasi intenda "e" nel senso di "e poi", nel qual caso le due frasi assumono significati ben diversi. Usando peró "$\wedge$" anziché "e", decidiamo di fare riferimento solamente alle tavole di verità escludendo quindi il significato "e poi".

Il seguente esempio illustra le tavole delle congiunzione e della disgiunzione. Ricordiamo che il valore assoluto $|x|$ di un numero reale x è uguale ad x se $x \geq 0$ ed è uguale a $-x$ se $x < 0$.

ESEMPIO 1.5. Siano x, y numeri reali.

(1) La proposizione "$xy = 0$" equivale a "$(x = 0) \vee (y = 0)$".
(2) La proposizione "$|x| = 3$" equivale a "$x = 3 \vee x = -3$".
(3) La proposizione "$|x| < 3$" equivale a "$-3 < x \wedge x < 3$".

ESERCIZIO 1.6. Siano a, b, c tre espressioni numeriche e supponiamo di sapere che $a \geq b$. La condizione aggiuntiva $b \geq c$ è sufficiente per poter concludere $a \geq c$? È anche necessaria?

SOLUZIONE: $b \geq c$ è sufficiente, ma non necessaria: infatti, fermo restando che $a \geq b$, la tesi $a \geq c$ potrebbe essere vera anche se b non fosse maggiore o uguale a c (ad esempio $a = 10, c = 5, b = 4$). In generale vale l'implicazione $(a \geq b \wedge b \geq c) \to a \geq c$, ma non l'implicazione inversa. □

ESEMPIO 1.7. $xy = 0$ equivale a $(x = 0) \vee (y = 0)$, ma in generale non equivale a $(x = 0) \oplus (y = 0)$. Infatti se $x = y = 0$ abbiamo che $xy = 0$ è vera mentre $(x = 0) \oplus (y = 0)$ è falsa.

Sebbene in generale un enunciato della forma $A \oplus B$ non equivalga a $A \vee B$ (in quanto la prima è vera e la seconda è falsa nel caso in cui A, B siano entrambi veri) è tuttavia possibile che ulteriori informazioni mi portino a restringere l'insieme dei casi che si possono verificare (dai quattro possibili a priori) e a stabilire l'equivalenza. Il seguente esempio chiarirà la situazione.

ESEMPIO 1.8. Dati due numeri reali x, y le seguenti proposizioni sono equivalenti:

(1) $x \leq 3$;
(2) $(x < 3) \vee (x = 3)$;
(3) $(x < 3) \oplus (x = 3)$.

Infatti se $x \leq 3$, allora o $x < 3$ o $x = 3$, e chiaramente non valgono entrambe le alternative. Quindi la (1) equivale alla (3). D'altra parte equivale anche alla (2) in quanto l'unico caso in cui $(x < 3) \vee (x = 3)$ potrebbe non essere equivalente a $(x < 3) \oplus (x = 3)$ sarebbe quello in cui le due proposizioni $x < 3$ ed $x = 3$ risultassero entrambe vere, ma questo, comunque si scelga x, è impossibile (stiamo naturalmente dando per note queste proprietà del $<$).

5. Basi di connettivi

Il seguente esempio mostra che possiamo ottenere il connettivo $\vee$ a partire da $\to, \neg$.

ESEMPIO 1.9. Date due proposizioni A e B le seguenti proposizioni si equivalgono.

(1) $\neg A \to B$;
(2) $A \vee B$;
(3) $\neg B \to A$".

Ad esempio: "Se non è zuppa è pan bagnato" equivale a: "O è zuppa o è pan bagnato", ed anche a "Se non è pan bagnato è zuppa". Altro esempio: "O mangi questa minestra o salti dalla finestra" equivale a "Se non mangi questa minestra salti dalla finestra".

Osservazione 1.10. Nello scrivere le formule dell'esempio precedente abbiamo omesso le parentesi seguendo la convenzione $\neg$ lega maggiormente degli altri connettivi e pertanto $\neg A \to B$ significa $(\neg A) \to B$ anziché $\neg(A \to B)$ (se avessimo voluto intendere la seconda formula avremmo dovuto mettere le parentesi). In generale per risparmiare parentesi seguiremo la convenzione che $\to$ lega meno di tutti gli altri connettivi. Ad esempio $A \wedge B \to C$ è da intendersi come $(A \wedge B) \to C$.

Analogamente possiamo ottenere $\to$ a partire da $\vee, \neg$.

Esempio 1.11. Date due proposizioni A e B le seguenti proposizioni si equivalgono:
(1) $A \to B$;
(2) $\neg A \vee B$;
Ad esempio "se son rose fioriranno" equivale a "o non sono rose o fioriranno".

In presenza del $\neg$ possiamo ottenere $\to$ a partire da $\wedge$ e viceversa.

Esempio 1.12. (1) $A \to B$ equivale a $\neg(A \wedge \neg B)$.
(2) $\neg(A \to \neg B)$ equivale a $(A \wedge B)$.
Come esempio della (2) sia $A =$ dormo, $B =$ piglio pesci. La proposizione "non è vero che se dormo non piglio pesci" equivale a "dormo e piglio pesci".

Esempio 1.13. $A \leftrightarrow B$ equivale a $(A \to B) \wedge (B \to A)$.

Esempio 1.14. La disgiunzione esclusiva può essere espressa usando gli altri connettivi: $A \oplus B$ equivale a $(A \vee B) \wedge \neg(A \wedge B)$.

6. Equivalenze notevoli

Per semplificare espressioni complicate possono far comodo le seguenti equivalenze.

Esempio 1.15. Date tre proposizioni p, q, r valgono le seguenti equivalenze:

- Leggi di idempotenza:
  $p \wedge p \equiv p$;
  $p \vee p \equiv p$;
- Legge della doppia negazione:
  $\neg(\neg p) \equiv p$;
- Leggi commutative:
  $p \wedge q \equiv q \wedge p$;
  $p \vee q \equiv q \vee p$;
- Leggi associative:
  $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$;
  $(p \vee q) \vee r \equiv p \vee (q \vee r)$;
- Leggi distributive:
  $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$;
  $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$;
- Leggi di De Morgan:
  $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$;
  $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$;
- Leggi di assorbimento:
  $p \vee (p \wedge q) \equiv p$,
  $p \wedge (p \vee q) \equiv p$.

7. Esercizi vari

ESEMPIO 1.16. Sia t una proposizione vera, e sia f una proposizione falsa. Valgono le seguenti equivalenze:

- $t \wedge p \equiv p$;
- $t \vee p \equiv t$;
- $f \wedge p \equiv f$;
- $f \vee p \equiv p$;
- $p \wedge \neg p = f$;
- $p \vee \neg p = t$.

8. Esercizi

ESERCIZIO 1.17. Ricordiamo che (a, b) è l'insieme dei numeri reali nell'intervallo compreso tra a e b (estremi esclusi). Usando le leggi di De Morgan esprimere la negazione di $x \in (a, b)$.

SOLUZIONE: $x \in (a, b)$ significa $a < x \wedge x < b$. La sua negazione $\neg(x \in (a, b))$ (che si può anche scrivere $x \notin (a, b)$) equivale a $\neg(a < x) \vee \neg(x < b)$, cioè $x \leq a \vee b \leq x$. □

ESERCIZIO 1.18. Usando le leggi di De Morgan esprimere la negazione di $|x| = 3$.

SOLUZIONE: $|x| = 3$ significa $x = 3 \vee x = -3$. La sua negazione $\neg(|x| = 3)$ equivale a $x \neq 3 \wedge x \neq -3$. (Dove $x \neq y$ sta per $\neg(x = y)$.) □

ESERCIZIO 1.19. Nel dominio dei numeri reali $a < b$ implica $4ab < (a + b)^2$.
Suggerimento: Conviene ragionare "all'indietro", cioè partiamo dalla conclusione e vediamo da cosa è implicata.

ESERCIZIO 1.20. Quali implicazioni valgono tra:

1. $(a \geq c) \wedge (b \geq d)$
2. $a + b \geq c + d$

SOLUZIONE: la prima implica la seconda. La seconda non implica sempre la prima. Ad esempio se $a = 10, b = 3, c = 4, d = 5$ la seconda è vera ma la prima è falsa. □

ESERCIZIO 1.21. Trovare una formula equivalente a $x \geq |y|$ che non usi la funzione modulo.

SOLUZIONE: $x \geq |y|$ equivale a $(y \geq 0 \wedge x \geq y) \vee (y < 0 \wedge x \geq -y)$. □

ESERCIZIO 1.22. Esprimere la relazione $x^2 \geq y^2$ senza usare i quadrati.

SOLUZIONE: Equivale a $|x| \geq |y|$, che a sua volta equivale a $x \geq |y| \vee x \leq -|y|$, che a sua volta equivale a $(y \geq 0 \wedge x \geq y) \vee (y \leq 0 \wedge x \geq -y) \vee (y \geq 0 \wedge x \leq -y) \vee (y \leq 0 \wedge x \leq y)$. Disegnare le regioni corrispondenti sul piano degli assi coordinati x, y. □

ESERCIZIO 1.23. Trovare le formule equivalenti:

1. $\frac{1}{3}x^3 \geq 3x^2$
2. $x \geq 9$
3. $x \geq 9 \vee x = 0$
4. $x \neq 0 \to x \geq 9$

Stabilire inoltre quali implicazioni valgono tra le formule considerate.

SOLUZIONE: $x \geq 9$ implica $\frac{1}{3}x^3 \geq 3x^2$ ma non viceversa.

La formula $\frac{1}{3}x^3 \geq 3x^2$ equivale a $x \geq 9 \vee x = 0$. Infatti se prendiamo $x = 0$ sono entrambe vere. Anche nel caso $x \geq 9$ sono entrambe vere. Nel rimanente caso, ovvero per x minore di 9 ma diverso da zero, sono entrambe false.

Analogamente si stabilisce che la prima, la terza e la quarta sono equivalenti, e sono tutte e tre implicate dalla seconda. E ovviamente ogni formula implica anche se stessa. □

ESERCIZIO 1.24. Esprimere i seguenti enunciati usando la relazione d'ordine $\geq$ e i connettivi ma senza usare max e min: $x \geq \max\{a, b\}$, $x \geq \min\{a, b\}$, $\max\{a, b\} \geq \max\{c, d\}$, $\max\{a, b\} \geq \min\{c, d\}$, $\min\{a, b\} \geq \max\{c, d\}$, $\min\{a, b\} \geq \min\{c, d\}$.

9. Tautologie

Le proposizioni

$$\neg(\text{piove} \vee \text{ tira vento}) \tag{1}$$
$$\neg((2 > 3) \vee (5 \leq 4)) \tag{2}$$
$$\neg((3 > 2) \vee (4 \leq 5)) \tag{3}$$

hanno tutte e tre la stessa *forma logica*, ovvero sono tutte della forma

$$\neg(A \vee B)$$

ma la prima potrebbe essere vera o falsa a seconda delle condizioni atmosferiche, la seconda è vera, e la terza è falsa. Come è evidente da questo esempio in generale la verità o falsità di una proposizione dipende dal suo contenuto, e non solo dalla sua forma logica. Ci sono però alcune proposizioni, chiamate *tautologie*, che sono vere semplicemente in virtù della loro forma logica, ovvero del modo in cui sono composte a partire da proposizioni più semplici usando i connettivi booleani. Diamo ora le definizioni precise.

DEFINIZIONE 1.25. Una **formula proposizionale** è una espressione costruito a partire da certe *variabili proposizionali* $A, B, C, \ldots$ i connettivi $\neg, \wedge, \vee, \to, \leftrightarrow$, e le parentesi, nel modo seguente. Ciascuna variabile proposizionale $A, B, C, \ldots$ è essa stessa una formula proposizionale, e se ϕ e ψ sono formula proposizionali lo sono anche $\neg\phi$, $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \to \psi)$, $(\phi \leftrightarrow \psi)$. Niente altro è una formula proposizionale se non ciò che si ottiene con una applicazione ripetuta di queste regole.

Da ciascuna formula proposizionale possiamo ottenere infinite proposizioni, tutte della stessa forma logica, sostituendo le variabili proposizionali con proposizioni vere e proprie. Ad esempio, come abbiamo visto, la proposizione $\neg(\text{piove} \vee \text{tira vento})$ ha come forma logica la formula proposizionale $\neg(A \vee B)$.

DEFINIZIONE 1.26. Una formula proposizionale ϕ si dice una **tautologia** se è vera per ogni valore delle sue variabili, cioè otteniamo una proposizione vera comunque sostituiamo delle proposizioni al posto delle sue variabili. Una formula proposizionale ϕ è **contraddittoria** se è falsa per ogni valore delle sue variabili, ovvero se la sua negazione ϕ è una tautologia.

Ad esempio $A \vee \neg A$ è una tautologia, in quanto risulta vera sia nel caso in cui A è una proposizione vera, sia nel caso in cui A è una proposizione falsa. La formula $A \wedge \neg A$ è invece contraddittoria. la formula $\neg(A \vee B)$ non è nè tautologica nè contraddittoria. Un altro esempio di tautologia è $((A \to B) \wedge \neg B) \to \neg A$. Usando le tavole si vede infatti facilmente che essa risulta vera nei quattro possibili casi per i valori di A e B (A vera e B vera, A vera e B falsa, A falsa e B vera, A falsa e B falsa).

Osservazione 1.27. Un metodo per riconoscere se una formula con n variabili proposizionali è una tautologia è quello di considerare i 2^n possibili casi per i valori di verità delle sue variabili e verificare usando le tavole che in ognuno dei casi la proposizione composta che ne risulta è vera. Esistono altri metodi per controllare se una formula è una tautologia, ma tutti i metodi noti richiedono una quantità di passaggi esponenziale al crescere del numero delle variabili. Il problema di stabilire se esistano metodi più efficienti (che permettano di riconoscere le tautologie in tempo polinomiale anziché esponenziale) è tuttora irrisolto.

Una proposizione ottenuta per sostituzione da una tautologia sarà anch'essa detta tautologia, e una proposizione ottenuta per sostituzione da una formula proposizionale contraddittoria sarà essa stessa detta contraddittoria. Ad esempio la proposizione "piove$\vee$ $\neg$piove" è una tautologia essendo ottenuta per sostituzione dalla tautologia $A\vee\neg A$. Come si vede da questo esempio una tautologia ha contenuto informativo nullo. Affermare "piove o non piove" non ci dà alcuna informazione sul fatto se piova o meno. In generale un enunciato che esprime una tautologia è vero a prescindere dalla verità o falsità degli enunciati elementari che lo costituiscono, e quindi non comunica nulla riguardo alla verità o falsità di questi ultimi.

Visto che non comunicano informazione, è lecito domandarsi a cosa servano le tautologie. Una possibile risposta è che esse giocano un ruolo importante nelle dimostrazioni. Consideriamo il seguente esempio:

Esempio 1.28. Consideriamo la seguente argomentazione logica: "L'assassino è il professore o l'assessore. Ma non è l'assessore. Quindi è il professore." Per condurre il ragionamento, cioè per mostrare che la tesi è implicata logicamente delle premesse, abbiamo implicitamente utilizzato la tautologia $((A \vee B) \wedge \neg B) \to A$, applicandola al caso in cui A sta per "l'assassino è il professore", e B sta per "l'assassino è l'assessore".

Esempio 1.29. Diamo altri schemi di ragionamento per tautologie. Per gli "esperti" abbiamo asteriscato le regole che possono portare a "dimostrazioni non costruttive".

- (Modus ponens) Da A e $A \to B$ posso ottenere B.
- (Taglio) Da $A \to B$ e $B \to C$ posso ottenere $A \to C$ (la formula B viene "tagliata").
- (Terzo escluso*) Da $A \to B$ e $\neg A \to B$, posso ottenere B. (Il nome "terzo escluso" deriva dal fatto che i due casi A e $\neg A$ esauriscono tutte le possibilità.)
- (Altra forma del terzo escluso*) Posso inserire $A \vee \neg A$ in qualunque punto di una dimostrazione.
- (Ragionamento per assurdo*) Conveniamo di indicare con $\perp$ una proposizione contraddittoria, come ad esempio una proposizione della forma $q \wedge \neg q$. La regola dell'assurdo dice che da $\neg p \to \perp$ posso ottenere p.
- (Negazione) Da $p \to \perp$ posso ottenere $\neg p$.
- (Doppia negazione*) Da $\neg\neg p$ posso ottenere p.
- (Ex falso quod libet) Da $\perp$ posso ottenere qualunque altra proposizione.
- (Contronominale) Da $A \to B$ posso ottenere $\neg B \to \neg A$.
- Da $A \to (B \to C)$ posso ottenere $(A \wedge B) \to C$.
- Da $(A \wedge B) \to C$ posso ottenere $A \to (B \to C)$.

CAPITOLO 2

Predicati e quantificatori

1. Predicati

Un **predicato** P associa a ciascun elemento x di di un dato dominio Ω di oggetti una proposizione $P(x)$, che può essere vera o falsa. Ad esempio se P è il predicato "essere un numero primo" ed x è un numero, allora $P(x)$ è la proposizione "x è un numero primo". Useremo anche il termine "**relazione**" come sinonimo di "predicato". Il termine relazione suggerisce una pluralità di soggetti che per l'appunto stanno in relazione, e quindi verrà impiegato preferibilmente per i predicati a più argomenti. Ad esempio il predicato "è minore di" tra numeri reali associa a ciascuna coppia ordinata (x, y) di numeri reali la proposizione "$x < y$", che sarà ovviamente vera o falsa a seconda di come si scelgono x ed y.

2. Quantificatore universale ed esistenziale

Introduciamo ora il quantificatore universale $\forall$ ("per ogni") e il quantificatore esistenziale $\exists$ ("esiste"). Se P è un predicato unario, la proposizione $(\exists x \in \Omega)\ P(x)$ esprime il fatto che esiste almeno un oggetto x nel dominio Ω che verifica il predicato, ovvero tale che valga $P(x)$. La proposizione $(\forall x \in \Omega)\ P(x)$ dice che per tutti gli oggetti x del dominio Ω vale $P(x)$. La "x" è una variabile "muta", ovvero al posto di "x" possiamo usare "y" o qualunque altra variabile senza cambiare il significato dell'espressione: dire che per tutti gli x vale $P(x)$ è la stessa cosa che dire che per tutti gli y vale $P(y)$. Valgono dunque le equivalenze

Fatto 2.1.

$$(\forall x \in \Omega)\ P(x) \equiv (\forall y \in \Omega)\ P(y)$$
$$(\exists x \in \Omega)\ P(x) \equiv (\exists y \in \Omega)\ P(y).$$

Se il dominio Ω su cui variano le variabili è sottinteso o irrilevante possiamo scrivere semplicemente $\forall x P(x)$ al posto di $(\forall x \in \Omega)\ P(x)$ ed $\exists x P(x)$ al posto di $(\exists x \in \Omega)\ P(x)$.

Esempio 2.2. Sia $\mathbb{R}$ l'insieme dei numeri reali. Dato un numero reale x, la proposizione $x^2 \geq 0$ è sempre vera. Per esprimere questo fatto scriviamo

$$(\forall x \in \mathbb{R})(x^2 \geq 0)$$

o semplicemente

$$\forall x(x^2 \geq 0)$$

se sottintendiamo che x vari in $\mathbb{R}$.

Esempio 2.3. Consideriamo l'equazione $2x = 1$. Tale equazione ha soluzione nel dominio $\mathbb{R}$ dei numeri reali (basta prendere $x = 1/2$), ma non nel dominio $\mathbb{Z}$ dei numeri interi (perché l'unica soluzione $1/2$ non è intera). Possiamo dunque affermare che

$$(\exists x \in \mathbb{R})(2x = 1)$$

ma non che

$$(\exists x \in \mathbb{Z})(2x = 1).$$

Quest'ultimo enunciato è falso, ed è pertanto vera la sua negazione

$$(\neg\exists x \in \mathbb{Z})(2x = 1),$$

la quale si può anche esprimere scrivendo

$$(\forall x \in \mathbb{Z})(2x \neq 1),$$

ovvero "per ogni intero x, $2x$ è diverso da 1".

In generale le negazioni trasformano i $\forall$ in $\exists$ e viceversa secondo le seguenti regole, il cui significato intuitivo dovrebbe essere chiaro:

FATTO 2.4.

$$\begin{aligned} \neg\forall x P(x) &\equiv \exists x \neg P(x) \\ \neg\exists x P(x) &\equiv \forall x \neg P(x) \end{aligned}$$

Ad esempio dire "non tutte le ciambelle riescono col buco" equivale a "esiste una ciambella senza buco", e "non c'è rosa senza spine" equivale a "tutte le rose hanno le spine".

OSSERVAZIONE 2.5. Si noti che se Ω è vuoto, $(\forall x \in \Omega)\ P(x)$ è sempre vero. Per convincersene osserviamo che la sua negazione equivale alla proposizione $(\exists x \in \Omega)\ \neg P(x)$, che è chiaramente falsa se Ω è vuoto. Ad esempio: "tutti gli unicorni bevono caffè" è una proposizione vera per il semplice fatto che gli unicorni non esistono e quindi non è possibile trovare un unicorno che non beva caffè. Quindi in generale non possiamo dire che $(\forall x \in \Omega)\ P(x) \Longrightarrow (\exists x \in \Omega)\ P(x)$ a meno di non sapere che Ω è non vuoto.

Per predicati in più variabili possiamo quantificare separatamente ciascuna variabile.

ESEMPIO 2.6. Per esprimere il fatto che $(x+y)^2 = x^2+2xy+y^2$ è sempre vera, ovvero che vale per qualsiasi scelta di x, y (numeri reali), usiamo due quantificatori universali:

$$\forall x \forall y((x+y)^2 = x^2 + 2xy + y^2)$$

che possiamo anche abbreviare con

$$\forall x, y((x+y)^2 = x^2 + 2xy + y^2)$$

In generale possiamo scambiare l'ordine dei quantificatori se sono tutti universali o tutti esistenziali:

FATTO 2.7.

$$\begin{aligned} \forall x \forall y P(x,y) &\equiv \forall y \forall x P(x,y) \\ \exists x \exists y P(x,y) &\equiv \exists x \exists y P(x,y) \end{aligned}$$

Più complicato è il caso in cui abbiamo una alternanza di quantificatori $\forall$ ed $\exists$ come ad esempio in $\forall x \exists y P(x,y)$. Un enunciato di questa forma significa che per ogni x vale la proposizione $\exists y P(x,y)$, ovvero per ogni x è possibile trovare un y, che in generale dipenderà da x, che verifica $P(x,y)$. Se alteriamo l'ordine dei quantificatori il significato cambia: $\exists y \forall x P(x,y)$ significa che è possibile trovare un y che va bene per tutti gli x, ovvero esiste un y tale che $\forall x P(x,y)$.

ESEMPIO 2.8. Se il dominio delle variabili è un insieme di persone, e $P(x,y)$ è la relazione "y è la mamma di x", $\forall x \exists y P(x,y)$ dice che ogni persona ha una mamma, mentre $\exists y \forall x P(x,y)$ asserisce l'esistenza di una persona y che è la mamma di tutti (inclusa se stessa).

Esempio 2.9. La proposizione

$$\forall x \exists y (y > x)$$

esprime il fatto che, dato un x, esiste un y (che dipende da x) tale che $y > x$. Nel dominio dei numeri reali tale proposizione è vera: basta prendere $y = x + 1$. La proposizione

$$\exists y \forall x (y > x)$$

esprime invece l'esistenza di un elemento y che verifichi la condizione $\forall x(y > x)$, ovvero che è maggiore di ogni numero reale. Tale proposizione è ovviamente falsa.

Per comprendere il significato di una proposizione complessa conviene prima decifrare le proposizioni più semplici contenute al suo interno per poi risalire via via verso l'esterno. Lo stesso procedimento si può adottare nel momento in cui si tratta si scrivere una formula complessa (anziché leggerla). Il seguente esempio chiarirà cosa intendiamo dire.

Esempio 2.10. Data una costante c consideriamo l'equazione $cx = 1$. Chiediamoci se l'equazione abbia una soluzione x (reale), ovvero se valga $\exists x(cx = 1)$. La risposta è positiva a condizione che $c \neq 0$: basta prendere $x = 1/c$. Vale quindi l'implicazione $c \neq 0 \to \exists x(cx = 1)$. Questa implicazione è vera per ogni valore di c (anche $c = 0$ visto che una implicazione con premessa falsa è vera), e possiamo quindi affermare

$$\forall c(c \neq 0 \to \exists x(cx = 1)).$$

Abbiamo costruito con poca fatica una proposizione con due quantificatori partendo dall'interno.

La comprensione di una proposizione con tre quantificatori alternati può essere difficile. Ad esempio $\forall x \exists y \forall z P(x, y, z)$ significa che per ogni a vale la proposizione $\exists y \forall z P(a, y, z)$, la quale a sua volta significa che esiste un b, in generale dipendente da a, che verifica la proposizione $\forall z P(a, b, z)$, la quale a sua volta significa che per ogni c vale $P(a, b, c)$. Anche in questo caso conviene partire dall'interno, e cercare di capire prima di tutto cosa significhi $\forall z P(a, b, z)$ (dipenderà ovviamente da chi è P).

3. Ambito di quantificazione

Dato un numero intero x, scriviamo $P(x)$ per "x è pari" e $Q(x)$ per "x è dispari". La proposizione $\exists x P(x)$ dice "esiste un numero pari" e la proposizione $\exists x Q(x)$ dice "esiste un numero dispari". Si tratta di due proposizioni vere, e pertanto lo è anche la loro congiunzione $\exists x P(x) \wedge \exists x Q(x)$. Ciò è ben diverso dal dire $\exists x(P(x) \wedge Q(x))$, la quale invece afferma l'esistenza di un x che verifica $P(x) \wedge Q(x)$, ovvero l'esistenza di un numero che è sia pari che dispari, cosa ovviamente falsa. Riepilogando:

Osservazione 2.11. In generale, dati due predicati P e Q, l'enunciato

$$\exists x P(x) \wedge \exists x Q(x) \tag{1}$$

non equivale a

$$\exists x(P(x) \wedge Q(x)). \tag{2}$$

L'enunciato (1) è la congiunzione di $A = \exists x P(x)$ e $B = \exists x Q(x)$, e poiché $\exists x Q(x)$ equivale a $\exists y Q(y)$, abbiamo

$$(1) \equiv \exists x P(x) \wedge \exists y Q(y).$$

La cosa importante da osservare è che $\exists x P(x) \wedge \exists x Q(x)$ è la *congiunzione* di due enunciati e quindi dal punto di vista sintattico va considerato come un enunciato che "inizia" con un $\wedge$, ovvero $\wedge$ è il suo "connettivo principale" (anche se tipograficamente inizia con un $\exists$). All'interno di $\exists x P(x) \wedge \exists x Q(x)$ si trovano due enunciati con un $\exists$ come connettivo principale, il primo è $\exists x P(x)$ e il secondo è $\exists x Q(x)$. La regola generale è che l'*ambito* di un quantificatore è limitato all'enunciato di cui lui è il connettivo principale, ovvero il quantificatore non agisce sulle variabili al di fuori del suo ambito.

CAPITOLO 3

Dimostrazioni e regole di inferenza

Abbiamo visto che lo scopo di una dimostrazione è quello di convincere qualcuno, ma soprattutto sé stessi, che una certa tesi segue da certe ipotesi. Diamo alcune regole generali per scrivere le dimostrazioni. Di alcune ne abbiamo già parlato in precedenza ma è bene riassumerle in forma sintetica.

1. Introduzione e scaricamento di una ipotesi

Ne abbiamo già parlato nella sezione 3 e basterà quindi uno schema sintetico:

Passaggi vari della dimostrazione D Assumiamo p (inizio della sottodimostrazione D') Passaggi vari q Quindi $p \to q$, scaricando l'ipotesi p (ritorno a D).

2. Ragionamento per tautologie:

Ne abbiamo già accennato nella sezione 9. La regola generale è la seguente. Se ϕ è una tautologia posso inserire ϕ in qualunque punto di una dimostrazione. Se $\phi \to \psi$ è una tautologia, e se nel corso di una dimostrazione ho ottenuto ϕ, posso ottenere ψ. Più in generale se $(\phi_1 \wedge \ldots \wedge \phi_n) \to \psi$ è una tautologia, e se ho ottenuto $\phi_1, \ldots, \phi_n$, posso ottenere ψ. Detto in altri termini: se ho ottenuto $\phi_1, \ldots, \phi_n$ e in base alle tavole di verità riesco a mostrare che in tutti i casi in cui sono vere $\phi_1, \ldots, \phi_n$ è vera anche ψ, allora posso ottenere ψ.

3. Uguaglianza

Dato a, posso inserire $a = a$ in qualunque punto di una dimostrazione.

Vale inoltre la regola di sostituzione (vedi sezione 1.1): Da $a = b$ e $P(a)$ posso dedurre $P(b)$. In forma schematica:

$$\frac{a = b,\ P(a)}{P(b)}$$

La regola va interpretata nel senso che posso sostituire *qualche* occorrenza di a con b ma non è necessario sostituirle *tutte*. Ad esempio da $a = b$ e $Q(a, a)$ posso dedurre $Q(a, b)$.

L'equivalenza tra proposizioni è equiparata ad una uguaglianza: da $A \leftrightarrow B$ e $C[A]$ posso dedurre $C[B]$, dove $C[A]$ è una proposizione complessa contenente A al suo interno. Anche in questo caso si intende che possiamo sostituire *qualche* A con B, non necessariamente tutte.

4. Assiomi

In qualunque punto di una dimostrazione posso inserire le proposizioni che decido di "dare per buone". Chiameremo tali proposizioni "assiomi". Tecnicamente gli assiomi possono essere pensati come ipotesi generali che decidiamo di non scaricare mai.

In una dimostrazione "formale" è necessario specificare gli assiomi una volta per tutte e non si può dare per buono assolutamente nulla che non sia stato preventivamente inserito nella lista degli assiomi. Tuttavia nelle dimostrazione informali saremo più rilassati e ci riserveremo la possibilità di inserire, via via che se ne presenti la necessità, tutto ciò che riteniamo di poter dare per buono. Ad esempio si può decidere di dare per buono che $2 + 2 = 4$ e dedurne che $3 \cdot (2 \cdot 2) = 3 \cdot 4$ in base alla regola di sostituzione. Oppure, supponendo di aver ottenuto due proposizioni della forma "$(k \geq 6) \to B$" e "$(k < 6) \to B$, posso ottenere B in base ad un ragionamento per tautologie dando per buono che $k \geq 6$ equivalga alla negazione di $k < 6$.

5. Regole per i quantificatori

5.1. Esistenza costruttiva. Da $P(a)$ posso ottenere $\exists x P(x)$.

5.2. Esistenza non costruttiva. Da $\neg\forall x P(x)$ posso ottenere $\exists x \neg P(x)$.

5.3. Particolarizzazione. Da $\forall x P(x)$ posso ottenere $P(a)$, dove a è una qualunque espressione che abbia senso sostituire al posto di x. Ad esempio se x è una variabile di tipo "numero", a deve essere una espressione numerica (come $2 + 4$, o $k + 4$, etc.), possibilmente contenente altre variabili al suo interno.

5.4. Generalizzazione. Se ho ottenuto $P(a)$ per un a "generico", posso ottenere $\forall x P(x)$. Qui "generico" significa che a non deve comparire in alcuna ipotesi non ancora scaricata nel momento in cui ho ottenuto $P(a)$ (eventuali assiomi contano come ipotesi: quindi a non deve comparire negli assiomi). A livello intuitivo la regola è giustificata dal fatto che se sono riuscito ad arrivare a $P(a)$ senza fare alcuna ipotesi su a, nello stesso modo potevo arrivare a $P(x)$ per qualsiasi x.

ATTENZIONE: La regola *non* consente di dimostrare $P(a) \to \forall x P(x)$, ma solo di dimostrare $\forall x P(x)$ qualora si sia già riusciti a dimostrare $P(a)$ (con a generico).

5.5. Scelta di un elemento. Dopo aver ottenuto $\exists x P(x)$ si può proseguire la dimostrazione dicendo "sia a tale che $P(a)$", ovvero si introduce l'ipotesi $P(a)$. Se a partire da questa ipotesi su a si riesce ad ottenere una proposizione Q che non contiene a, si può a questo punto ottenere Q scaricando l'ipotesi.

In forma grafica:

$\exists x P(x)$
Introduzione dell'ipotesi $P(a)$ (inizio della sottodimostrazione D')
Passaggi vari
Q (siamo ancora in D')
Quindi Q, scaricando l'ipotesi $P(a)$ (ritorno alla dimostrazione principale).

A livello intuitivo la motivazione della regola è la seguente. Sapendo che esiste almeno un elemento che verifica P, posso immaginare di "sceglierne" uno e dargli come nome "a" (o un altro nome non precedentemente impiegato), e quindi l'ipotesi $P(a)$ è "gratuita", ovvero può essere effettuata "senza perdita di generalità" (per questo la posso poi scaricare a costo zero, ovvero senza introdurre implicazioni). Devo in ogni caso usare un nome "nuovo" per battezzare l'elemento scelto altrimenti potrei cadere in errore. Ad esempio

se P è un predicato numerico e so che $\exists x P(x)$, non posso dire che vale $P(4)$ perché questa sarebbe ovviamente una ipotesi restrittiva, ma posso invece supporre senza perdita di generalità che valga $P(a)$: se uso "a" non sto infatti nè affermando nè escludendo che a sia proprio il numero 4, come è giusto che sia in mancanza di informazioni a riguardo.

Esercizio 3.1. Cosa c'è di sbagliato nel seguente ragionamento? 2 è pari, quindi per la regola di generalizzazione tutti i numeri sono pari.

Soluzione: Per concludere che 2 è pari ho usato alcune proprietà di 2 che o compaiono negli assiomi (ad esempio ci potrebbe essere l'assioma definitorio $2 = 1 + 1$) o in altre ipotesi implicite "date per buone". Quindi 2 non può essere considerato come un elemento generico. □

Esercizio 3.2. Da $(\forall x(P(x) \to Q)$ e $\exists x P(x))$ ottengo Q.

Soluzione: Assumiamo $\forall x(P(x) \to Q)$ e $\exists x P(x)$. Sia a tale che $P(a)$. Per particolarizzazione abbiamo $P(a) \to Q$. Siccome abbiamo anche $P(a)$ otteniamo Q per tautologie. Quindi Q, scaricando l'ipotesi $P(a)$. □

Esercizio 3.3. Si mostri che, in presenza delle altre regole, la regola "scelta di un elemento" equivale alla regola espressa dall'esercizio precedente.

6. Equivalenze notevoli

Esercizio 3.4. Valgono le seguenti equivalenze:

$$\begin{array}{ccc}
\forall x P(x) & \equiv & \forall y P(y) \\
\exists x P(x) & \equiv & \exists y P(y) \\
\neg\forall x P(x) & \equiv & \exists x \neg P(x) \\
\neg\exists x P(x) & \equiv & \forall x \neg P(x) \\
\exists x(P(x) \vee Q(x)) & \equiv & \exists x P(x) \vee \exists x Q(x) \\
\forall x(P(x) \wedge Q(x)) & \equiv & \forall x P(x) \wedge \forall x Q(x) \\
\exists x P(x) \wedge \exists x Q(x) & \equiv & \exists x \exists y(P(x) \wedge Q(y)) \\
\forall x P(x) \vee \forall x Q(x) & \equiv & \forall x \forall y(P(x) \vee Q(y)) \\
\exists x(P(x) \wedge R) & \equiv & (\exists x P(x)) \wedge R \\
\forall x(P(x) \vee R) & \equiv & (\forall x P(x)) \vee R \\
\exists x(P(x) \vee R) & \equiv & (\exists x P(x)) \vee R \\
\forall x(P(x) \wedge R) & \equiv & (\forall x P(x)) \wedge R
\end{array}$$

dove "$P(x)$" sta per "x verifica il predicato P", "$Q(x)$" sta per "x verifica il predicato Q", e la proposizione R non dipende da x (ma potrebbe dipendente da altri parametri $z, w, \ldots$).

Esercizio 3.5.

$$(\exists x P(x)) \to Q \quad \equiv \quad \forall x(P(x) \to Q)$$

Per trovare altre equivalenze notevoli coinvolgenti l'implicazione e i quantificatori basta scrivere $A \to B$ nella forma equivalente $\neg A \vee B$ applicare le equivalenze precedentemente viste.

Esercizio 3.6.

$$\exists x(P(x) \to Q) \quad \equiv \quad (\exists x \neg P(x)) \vee Q)$$

Soluzione: La prima formula equivale a $\exists x(\neg P(x) \vee Q)$, che equivale (in quanto Q non dipende da x) a $(\exists x \neg P(x)) \vee Q$. □

Le equivalenze sopra viste sono sufficienti a spostare tutti i quantificatori verso l'esterno, come nell'esempio seguente:

Esercizio 3.7. Si dimostri l'equivalenza:

$$\exists x P(x) \to \exists y Q(y) \equiv \forall x \exists y (P(x) \to Q(y))$$

Tutte le formule che abbiamo scritto in questa sezione sono esempi di "formule predicative", ovvero espressioni costruite per mezzo dei connettivi e dei quantificatori a partire da certi simboli $P(-), Q, \ldots$ che rappresentano dei predicati o delle proposizioni. Una formula predicativa è *logicamente valida* se è sempre vera indipendentemente da quali predicati e proposizioni sostituiamo al posto di tali simboli (e dal dominio in cui variano le variabili, purchè non sia vuoto). Le regole dimostrative che abbiamo dato sono in linea di principio sufficienti a dimostrare tutte le formule predicative logicamente valide.

7. Esercizi vari

Esercizio 3.8. Formalizzare usando i connettivi logici e le operazioni e relazioni aritmetiche $+, \cdot, 0, 1, \leq$
x è primo.
x divide y.

Esercizio 3.9. Formalizzare: "Ogni coppia di interi positivi ha un massimo comun divisore".

Esempio 3.10. (Uno o due quantificatori) Determinare quali formule sono vere in $\mathbb{N}$ (cioè assumendo che il dominio delle variabili sia $\mathbb{N}$), quali in $\mathbb{Z}$, quali in $\mathbb{R}$.

$$\forall x (x \geq 0)$$
$$\exists x (x^2 > 3x)$$
$$\forall x (x^2 > 3x)$$
$$\forall x, y ((x+y)^2 = x^2 + 2xy + y^2)$$
$$\exists x, y ((x+y)^2 = x^2 + 2x + 1)$$
$$\forall x \forall y (x > y)$$
$$\exists x \exists y (x > y)$$
$$\forall x \exists y (x > y)$$
$$\exists y \forall x (x > y)$$
$$\forall x \exists y (x + y = 0)$$
$$\exists x \forall y (x + y = 0)$$
$$\forall x \exists y (xy = 1)$$
$$\exists x \forall y (xy = 1)$$
$$\exists x \forall y (xy = y)$$

Esempio 3.11. (Tre quantificatori) Determinare quali formule sono vere in $\mathbb{Z}$.

$$1. \forall x \exists y \forall z (x + y = z)$$
$$2. \exists x \forall y \exists z (x + y = z)$$
$$3. \forall x \exists y \forall z (z(x + y) = z)$$

Esempio 3.12. (Per chi conosce le funzioni) Data $f\colon \mathbb{R} \to \mathbb{R}$, formalizzare usando i quantificatori: f è iniettiva. f è crescente. f è surgettiva. f è limitata. f è continua in 0, f è continua in tutti i punti. Formalizzare poi la negazione di ognuna spingendo le negazioni all'interno.

CAPITOLO 4

Insiemi

1. Appartenenza e notazioni

Un **insieme** è una qualsiasi collezione di oggetti. Ad esempio possiamo considerare l'insieme degli studenti di una data classe. Scriviamo $x \in A$ per indicare il fatto che l'oggetto x **appartiene** all'insieme A, cioè A contiene x come elemento. Per indicare il fatto che x non appartiene ad A scriviamo $\neg(x \in A)$ o per brevità $x \notin A$.

Indicheremo con il simbolo $\emptyset$ l'insieme vuoto, ossia l'insieme che non contiene nessun elemento. Per denotare un insieme si possono elencare tra parentesi graffe gli elementi dell'insieme oppure si può specificare una proprietà caratteristica degli elementi dell'insieme. Ad esempio $\{2, 3, 5, 7, 11\}$ è l'insieme dei numeri primi minori o uguali a 11, che si può scrivere anche nella forma $\{x \mid x \text{ è un numero primo } \leq 11\}$ (si legge: l'insieme degli x tali che x è un numero primo ≤ 11). In generale la barra verticale si può leggere "tale che" e la notazione $\{x \mid P(x)\}$ indica dunque l'insieme degli oggetti x che verificano la condizione $P(x)$. Dato un oggetto a, dire che $a \in \{x \mid P(x)\}$ è la stessa cosa che dire $P(a)$:

$$a \in \{x \mid P(x)\} \iff P(a).$$

Una variante di questa notazione è la seguente. Se A è un insieme, scriviamo $\{x \in A \mid P(x)\}$ per indicare l'insieme degli elementi x di A che verificano la condizione $P(x)$. Abbiamo quindi:

$$a \in \{x \in A \mid P(x)\} \iff (a \in A) \wedge P(a).$$

Spesso quando si usa la notazione $\{x \mid P(x)\}$ si sottintende che x vari all'interno di un insieme A prefissato. Ad esempio $\{x \mid x \text{ è un numero primo } \leq 11\}$ è la stessa cosa di $\{x \in \mathbb{N} \mid x \text{ è un numero primo } \leq 11\}$, dove $\mathbb{N}$ è l'insieme dei numeri naturali.

Esempio 4.1. Consideriamo l'insieme $A = \{\mathbb{N}, \{1, 2, 3\}, 4, +\}$. Si tratta di un insieme con 4 elementi ben distinti fra loro : l'insieme $\mathbb{N}$, l'insieme $\{1,2,3\}$, il numero 4 e il simbolo $+$. Dunque scriveremo:

$$\mathbb{N} \in A, \quad \{1, 2, 3\} \in A, \quad 4 \in A, \quad + \in A$$

Questi e solo questi sono gli elementi di A. Per esempio, non è vero che $1 \in A$, anche se $1 \in \mathbb{N}$ e $1 \in \{1, 2, 3\}$.

Due insiemi A, B sono uguali se hanno gli stessi elementi, ovvero, dato un oggetto qualunque x, vale la doppia implicazione $x \in A \leftrightarrow x \in B$. Ad esempio $\{11, 7, 5, 3, 2, \}$ è lo stesso insieme di $\{2, 3, 5, 7, 11\}$ anche se gli elementi sono elencati in modo diverso. Se scriviamo $\{11, 2, 3, 5, 7, 5\}$ otteniamo ancora una volta lo stesso insieme anche se il 5 è stato elencato due volte. Quando scriviamo un insieme nella forma $\{a, b, c, d, \text{etc.}\}$ l'unica cosa che conta è chi c'è e chi non c'è nell'elenco, l'ordine e le ripetizioni sono del tutto irrilevanti.

Esempio 4.2. Quanti diversi insiemi compaiono nella seguente lista?

$$\{1, 5, 4, 5\}, \{5, 4, 1\}, \{5, 5\}, \{5\}, \{1, 3, 4, 5\}, \{5, 4, 3, 1\}, \{1, 3, 6\}$$

SOLUZIONE: Nella lista compaiono quattro insiemi distinti fra loro: {5}, {5,4,1}, {1,3,6}, {5,4,3,1} . □

2. Stringhe

Non bisogna confondere gli insiemi con le **stringhe**, in cui a differenza che negli insiemi l'ordine e le ripetizioni contano. Ad esempio un numero di telefono non è un insieme di numeri ma è piuttosto una stringa di numeri. Per rendersene conto basta osservare che il numero di telefono 0502213261 è diverso da 0502213216, sebbene l'insieme delle cifre che vi compaiono sia lo stesso. Per indicare una stringa si possono usare le parentesi tonde anzichè le graffe: ad esempio il numero di telefono 0502213261 può essere identificato con la stringa $(0, 5, 0, 2, 2, 1, 3, 2, 6, 1)$, che è diversa da $(0, 5, 0, 2, 2, 1, 3, 2, 1, 6)$ sebbene l'insieme $\{0, 5, 0, 2, 2, 1, 3, 2, 6, 1\}$ sia uguale a $\{0, 5, 0, 2, 2, 1, 3, 2, 1, 6\}$ (entrambi sono uguali a $\{0, 5, 2, 1, 3, 6\}$).

Mentre per definire l'uguaglianza tra gli insiemi conta solo chi vi appartiene e chi no, per le stringhe conta anche l'ordine. In altre parole due stringhe sono uguali se hanno la stessa lunghezza, gli stessi primi elementi, gli stessi secondi elementi, eccetera.

ESEMPIO 4.3. Se vi si chiede di trovare tutti i valori x, y tali che $(1, 3) = (x, y)$ l'unica soluzione è $x = 1, y = 3$. Se invece vi si chiede di trovare tutti i valori x, y tali che $\{1, 3\} = \{x, y\}$ ci sono due soluzioni: $x = 1, y = 3$ oppure $x = 3, y = 1$ (in quanto $\{1, 3\}$ è uguale non solo a $\{1, 3\}$ ma anche a $\{3, 1\}$).

In generale per le stringhe di lunghezza due (dette anche coppie ordinate) vale il principio:

$$(a, b) = (c, d) \iff a = c \wedge b = d$$

mentre invece, per quanto appena visto, per gli insiemi non vale:

$$\{a, b\} = \{c, d\} \iff a = c \wedge b = d$$

Vale invece (esercizio..) che $\{a, b\} = \{c, d\}$ se e solo se $(a = c \wedge b = d) \vee (a = d \wedge b = c)$.

3. Il prodotto cartesiano

DEFINIZIONE 4.4. Dati due insiemi A e B, il prodotto cartesiano $A \times B$ è l'insieme di tutte le coppie ordinate in cui il primo elemento è un elemento di A e il secondo elemento è un elemento di B:

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

ESEMPIO 4.5. Il piano cartesiano con ascisse e ordinate è una rappresentazione del prodotto cartesiano $\mathbb{R} \times \mathbb{R}$ (abbreviato $\mathbb{R}^2$). Da questo potete capire bene come l'ordine sia importante per gli elementi di un prodotto cartesiano: per esempio il punto $(7, 5)$ nel piano è diverso dal punto $(5, 7)$.

ESEMPIO 4.6. Sia $A = \{1, 2, 3, 4, 5\}$ e sia $B = \{4, 5, 6, 7, 8, 9\}$. Allora $A \times B$ ha $30 = 5 \cdot 6$ elementi, perché è costituito da tutte le coppie in cui il primo elemento è un elemento di A (5 scelte) e il secondo elemento è un elemento di B (6 scelte). Elenchiamoli tutti:

$$(1, 4),\ (1, 5),\ (1, 6),\ (1, 7),\ (1, 8),\ (1, 9),\ (2, 4),\ (2, 5),\ (2, 6),\ (2, 7),\ (2, 8),\ (2, 9)$$
$$(3, 4),\ (3, 5),\ (3, 6),\ (3, 7),\ (3, 8),\ (3, 9),\ (4, 4),\ (4, 5),\ (4, 6),\ (4, 7),\ (4, 8),\ (4, 9)$$
$$(5, 4),\ (5, 5),\ (5, 6),\ (5, 7),\ (5, 8),\ (5, 9)$$

Notate che $(4, 5)$ e $(5, 4)$ sono due elementi distinti, e che $(4, 4)$ e $(5, 5)$ appartengono ad $A \times B$ visto che $4 \in A \cap B$ e $5 \in A \cap B$.

In generale, se l'insieme A ha n elementi e l'insieme B ha m elementi, il prodotto cartesiano $A \times B$ ha $n \cdot m$ elementi.

Osserviamo che se $A \neq B$ allora l'insieme $A \times B$ è diverso da $B \times A$ (anche se i due insiemi hanno lo stesso numero di elementi). Per convincersene, prendiamo di nuovo in considerazione gli stessi insiemi $A = \{1, 2, 3, 4, 5\}$ e $B = \{4, 5, 6, 7, 8, 9\}$ dell'esempio precedente; gli elementi di $B \times A$ sono sempre 30, ma sono:

$$(4,1),\ (4,2),\ (4,3),\ (4,4),\ (4,5),\ (5,1),\ (5,2),\ (5,3),\ (5,4),\ (5,5)$$

$$(6,1),\ (6,2),\ (6,3),\ (6,4),\ (6,5),\ (7,1),\ (7,2),\ (7,3),\ (7,4),\ (7,5)$$

$$(8,1),\ (8,2),\ (8,3),\ (8,4),\ (8,5),\ (9,1),\ (9,2),\ (9,3),\ (9,4),\ (9,5)$$

L'elemento $(8, 1)$, per esempio, appartiene a $B \times A$ ma non ad $A \times B$. L'intersezione $(A \times B) \cap (B \times A)$ è costituita solo da 4 elementi:

$$(A \times B) \cap (B \times A) = \{(4,4),\ (4,5),\ (5,4),\ (5,5)\}$$

La definizione di prodotto cartesiano si generalizza immediatamente al caso del prodotto di n insiemi:

Definizione 4.7. . Dati n insiemi (con $n \geq 2$) $A_1, A_2, \ldots, A_n$, il prodotto cartesiano $A_1 \times A_2 \times \cdots \times A_n$ è l'insieme di tutte le stringhe di n elementi in cui il primo elemento è un elemento di A_1, il secondo elemento è un elemento di A_2... e, in generale, l'i-esimo elemento è un elemento di A_i:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i\}$$

Esempio 4.8. Se $C = \{0, 1\}$, $D = \{2, 3\}$, $E = \{0\}$, $F = \{6, 7, 8, \}$, il prodotto cartesiano $C \times D \times F$ ha 12 elementi: $(0, 2, 6)$, $(0, 2, 7)$,$(0, 2, 8)$,$(0, 3, 6)$,$(0, 3, 7)$,$(0, 3, 8)$,$(1, 2, 6)$, $(1, 2, 7)$,$(1, 2, 8)$,$(1, 3, 6)$,$(1, 3, 7)$,$(1, 3, 8)$. Continuate l'esempio descrivendo i prodotti cartesiani

$$C \times D \times E, \quad C \times F \times F, \quad F \times F \times F.$$

4. Inclusione

Definizione 4.9. Dati due insiemi A, B diciamo che A è incluso in B, o che A è un sottoinsieme di B (e scriviamo $A \subseteq B$) se ogni elemento di A è anche elemento di B. L'inclusione $A \subseteq B$ può essere espressa usando i quantificatori nel modo seguente

$$\forall x\ (x \in A \to x \in B).$$

Si noti che $A = B$ se e solo se valgono le due inclusioni $A \subseteq B$ e $B \subseteq A$.

Osservazione 4.10. I seguenti enunciati sono equivalenti:

$$\{x \mid P(x)\} \subseteq \{x \mid Q(x)\} \tag{4.1}$$

$$\forall x\ (P(x) \to Q(x)) \tag{4.2}$$

Ad esempio dire che $\forall x\ (x \geq 9 \to x \geq 5)$ equivale a dire che la semiretta $\{x \mid x \geq 9\}$ è inclusa nella semiretta $\{x \mid x \geq 5\}$.

Osserviamo che, come conseguenza della Definizione 4.9 l'insieme vuoto $\emptyset$ è un sottoinsieme di ogni insieme. Infatti, riscriviamo la definizione con $A = \emptyset$; otteniamo che $\emptyset$ è un sottoinsieme di B se e solo se è vera:

$$z \in \emptyset \to z \in B$$

Una implicazione $p \to q$, come sappiamo, è vera solo nei seguenti casi:
1) p è falsa
2) p è vera e q è vera

Qui siamo nel caso 1), perché $z \in \emptyset$ è sempre una proposizione falsa, visto che $\emptyset$ non contiene nessun elemento.

Dunque qualunque sia l'insieme B che consideriamo, vale $\emptyset \subseteq B$.

ESEMPIO 4.11. Sia B l'insieme $\{1, \{2,3\}, \{4\}\}$. Tale insieme ha 3 elementi:

$$1 \in B, \quad \{2,3\} \in B, \quad \{4\} \in B$$

Dunque fra gli elementi c'è il numero 1 e l'insieme $\{4\}$ che è un insieme costituito da un solo elemento, il numero 4. Vorrei sottolineare che 4 e $\{4\}$ sono due oggetti diversi. Scrivere $\{4\} \in B$ è giusto, mentre scrivere $4 \in B$ è sbagliato. Quali sono i sottoinsiemi di B ? Sono 8, guardiamoli uno per uno:
– Uno è $\emptyset$, come sappiamo.
– Poi ci sono tre sottoinsiemi costituiti da un solo elemento di B: il sottoinsieme $\{1\}$, il sottoinsieme $\{\{2,3\}\}$ (notate che ci sono due parentesi graffe, perché $\{2,3\}$ è elemento di B, dunque il sottoinsieme che è costituito da tale elemento si indica con $\{\{2,3\}\}$) e il sottoinsieme $\{\{4\}\}$.
– Poi abbiamo i tre sottoinsiemi che sono costituiti da due elementi ciascuno: $\{1, \{2,3\}\}$, poi $\{1, \{4\}\}$, e infine $\{\{2,3\}, \{4\}\}$.
– Infine c'è l'insieme B stesso.

Per concludere con un esercizietto riassuntivo, provate a pensare cosa vogliono dire le seguenti proposizioni :

$$1 \in B,\ \{1\} \subseteq B,\ \{4\} \in B,\ \{\{4\}\} \subseteq B,\ 2 \notin B,\ 4 \notin B,\ \{2,3\} \not\subseteq B,\ \{2,3\} \in B$$

e verificate che sono tutte vere.

5. Le leggi per l'intersezione, l'unione e il complementare fra insiemi.

DEFINIZIONE 4.12. Dati A e B sottoinsiemi di un insieme universo Ω, definiamo:

- l'*intersezione* di A e B
$$A \cap B = \{x \in \Omega \mid x \in A \quad \wedge \quad x \in B\}$$
- l'*unione* di A e B
$$A \cup B = \{x \in \Omega \mid x \in A \quad \vee \quad x \in B\}$$
- la *differenza* A meno B
$$A - B = \{x \in \Omega \mid x \in A \quad \wedge \quad x \notin B\}$$
- il *complementare* di A in Ω
$$A^c = \{x \in \Omega \mid x \notin A\}$$

Queste operazioni insiemistiche obbediscono a delle regole che discendono direttamente dalle equivalenze notevoli per proposizioni elencate nell'Esempio 1.15:

TEOREMA 4.13. *Siano A, B, C sottoinsiemi di un insieme universo Ω. Allora valgono le seguenti identità:*

- *Leggi di idempotenza: $A \cap A = A$, $A \cup A = A$*
- *Legge della doppia negazione: $(A^c)^c = A$*

- *Leggi commutative:* $A \cap B = B \cap A$, $A \cup B = B \cup A$
- *Leggi associative:* $(A \cap B) \cap C = A \cap (B \cap C)$, $(A \cup B) \cup C = A \cup (B \cup C)$
- *Leggi distributive:* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- *Leggi di De Morgan:* $(A \cap B)^c = A^c \cup B^c$, $(A \cup B)^c = A^c \cap B^c$
- *Leggi di assorbimento:* $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$

DIMOSTRAZIONE. Le leggi contenute in questo teorema sono già automaticamente dimostrate se abbiamo dimostrato (con le tabelle di verità, per esempio) le corrispondenti equivalenze per proposizioni. Vediamo perché. Dimostriamo per esempio una delle leggi di De Morgan:

$$(A \cap B)^c = A^c \cup B^c$$

Sappiamo che per tre generiche proposizioni p, q, r vale la legge di De Morgan

$$\neg\,(p \wedge q) \equiv (\neg\, p)\ \vee\ (\neg\, q)$$

Dato un elemento x nell'universo Ω, scegliamo queste tre proposizioni: p:"$x \in A$", q:"$x \in B$", r:"$x \in C$". Applicata a queste tre proposizioni particolari, cosa ci dice la legge di De Morgan? Dice che

$$\neg\,(x \in A\ \wedge\ x \in B)$$

è equivalente a

$$\neg\,(x \in A)\ \vee\ \neg\,(x \in B)$$

Tradotto nel linguaggio degli insiemi questo significa che $x \in (A \cap B)^c$ è equivalente a $x \in A^c \cup B^c$. Dunque quando si sceglie un elemento x dell'universo Ω la sua appartenenza all'insieme $(A \cap B)^c$ è equivalente all'appartenenza all'insieme $A^c \cup B^c$. □

Naturalmente le leggi contenute nel teorema precedente si potrebbero dimostrare anche senza citare esplicitamente le leggi di equivalenza fra proposizioni. Per esercitare il nostro linguaggio, mostriamo con un esempio come si potrebbe procedere:

ESEMPIO 4.14 (Dimostrazione di una delle leggi distributive). Scriviamo la dimostrazione della prima delle due leggi, ossia

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Cominciamo col provare che

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$$

Per far questo dobbiamo dimostrare che se un elemento x di Ω appartiene a $A \cup (B \cap C)$ allora deve appartenere anche a $(A \cup B) \cap (A \cup C)$. In simboli:

$$x \in A \cup (B \cap C) \Longrightarrow x \in (A \cup B) \cap (A \cup C)$$

Infatti se un elemento x appartiene a $A \cup (B \cap C)$ allora vuol dire che $x \in A$ o $x \in B \cap C$. Se $x \in A$ allora $x \in A \cup B$ e $x \in A \cup C$, dunque $x \in (A \cup B) \cap (A \cup C)$ come volevamo dimostrare. Se $x \in B \cap C$ allora, visto che $x \in B$ e $x \in C$ di nuovo vale che $x \in A \cup B$ e $x \in A \cup C$, dunque $x \in (A \cup B) \cap (A \cup C)$.

Resta ora da far vedere che

$$A \cup (B \cap C) \supseteq (A \cup B) \cap (A \cup C)$$

Seguiamo come prima la strategia di mostrare che per un elemento $y \in \Omega$ vale

$$y \in (A \cup B) \cap (A \cup C) \Longrightarrow y \in A \cup (B \cap C)$$

Sia dunque $y \in A \cup B$ e $y \in A \cup C$. Perché queste due relazioni siano vere bisogna che $y \in A$ oppure, se ciò non è vero, allora deve essere $y \in B - A$ e $y \in C - A$. Nel primo

caso (ossia $y \in A$) segue subito che $y \in A \cup (B \cap C)$ come volevamo dimostrare. Nel secondo caso, $y \in B - A$ e $y \in C - A$ implica che $y \in B$ e $y \in C$ e dunque $y \in B \cap C$, da cui di nuovo segue subito $y \in A \cup (B \cap C)$.

Facciamo ancora un esercizio in cui compare una dimostrazione dello stesso stile.

ESERCIZIO 4.15. $A \subseteq U \ \wedge \ (A \cap (U \setminus B) = \emptyset) \Longrightarrow A \subseteq B$.

SOLUZIONE: Visto che dobbiamo dimostrare una implicazione cominciamo con l'assumerne la premessa $A \subseteq U \ \wedge \ (A \cap (U \setminus B)$ e cerchiamo di ottenere $A \subseteq B$. Ricordiamo che per definizione questo significa $\forall x(x \in A \to x \in B)$. Consideriamo quindi un generico oggetto x, assumiamo $x \in A$, e cerchiamo di dimostrare $x \in B$. Per le ipotesi fatte sappiamo che $A \subseteq U$, e quindi x deve appartenere ad U. Se per assurdo non appartenesse a B mettendo insieme tutto ciò che sappiamo su x avremmo $x \in A \cap (U \setminus B)$, contraddicendo l'ipotesi che tale insieme è vuoto. □

6. L'insieme delle parti

DEFINIZIONE 4.16. Dato un insieme A, l'insieme $\mathcal{P}(A)$ delle parti di A è l'insieme i cui elementi sono tutti i sottoinsiemi di A:

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Osserviamo in particolare che $A \in \mathcal{P}(A)$ e $\emptyset \in \mathcal{P}(A)$.
Per esempio, se $A = \{1, 2\}$, il suo insieme delle parti è costituito da 4 elementi:

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, A\}$$

Nel Paragrafo 4 (Esempio 4.11) abbiamo visto, contandoli uno per uno, che i sottoinsiemi di un insieme di tre elementi sono 8. Provate già da ora a intuire quanti sono gli elementi di $\mathcal{P}(A)$ se l'insieme di partenza A ha n elementi (discuteremo questa formula più avanti, nel Paragrafo 4 del Capitolo 7).

7. Esercizi

ESERCIZIO 4.17. Dati tre insiemi A, B, C in un universo Ω, consideriamo i seguenti insiemi:

$$X = A \cup B \cup C^c \ ; \quad Y = [(A^c \cap B^c) \cap (B \cup C)]^c \ ; \quad Z = (A \cup B) \cap (A \cup C) \ .$$

Dire se – qualunque sia la scelta di A, B, C – ci sono delle relazioni di inclusione fra gli insiemi X, Y, Z e anche se, in particolare, ci sono relazioni di uguaglianza.

SOLUZIONE: Per prima cosa usiamo le leggi di De Morgan per semplificare l'espressione che definisce Y:

$$Y = [(A^c \cap B^c) \cap (B \cup C)]^c = (A^c \cap B^c)^c \cup (B \cup C)^c =$$

ancora per De Morgan (e per la legge del doppio complementare)

$$= (A \cup B) \cup (B^c \cap C^c)$$

Usando la legge distributiva,

$$Y = (A \cup B) \cup (B^c \cap C^c) = (A \cup B \cup B^c) \cap (A \cup B \cup C^c)$$

Ora, $A \cup B \cup B^c$ è uguale all'insieme universo Ω e dunque abbiamo

$$Y = \Omega \cap (A \cup B \cup C^c) = A \cup B \cup C^c$$

Abbiamo a questo punto dimostrato che $Y = X$. Visto che Z e X si costruiscono a partire da $A \cup B$ ma nel caso di Z poi si prosegue con una intersezione e nel caso di X si prosegue con una unione (con C^c), si deduce che $Z \subseteq X = Y$. In generale non vale $Z = X$. □

Esercizio 4.18. Siano a, b numeri reali e consideriamo i seguenti insiemi:

(1) $A = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq a \wedge y \geq b\}$;
(2) $B = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq a \vee y \leq b\}$;
(3) $C = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq a \wedge y < b\}$.

(i) Quali inclusioni tra i tre insiemi sopra elencati valgono per ogni scelta di a, b?
(ii) Quali inclusioni sono certamente false per ogni scelta di a, b?

Soluzione: L'esercizio ci chiede di controllare se, per ogni scelta di a e b, sono vere o false le seguenti sei proposizioni:

$$A \subseteq B \quad A \subseteq C \quad B \subseteq A \quad B \subseteq C \quad C \subseteq A \quad C \subseteq B$$

Innanzitutto notiamo che, vale $A \subseteq B$. Infatti A è incluso nell'insieme $D = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq a\}$ mentre $D \subseteq B$. Anche C è incluso in D, dunque è vera $C \subseteq B$. Gli insiemi C e A sono disgiunti, ossia $A \cap C = \emptyset$: infatti, un elemento (x, y) che appartenesse ad $A \cap C$ dovrebbe soddisfare contemporaneamente $y \geq b$ e $y < b$, il che è impossibile. Visto che gli insiemi A e C non sono vuoti, sono dunque false $A \subseteq C$ e $C \subseteq A$. Restano da valutare $B \subseteq A$ e $B \subseteq C$. Per vedere che la prima è falsa, basta mostrare un elemento che appartiene a B ma non ad A, per esempio l'elemento $(a, b-1)$, oppure anche $(a-1, b-1)$. Quest'ultimo elemento $(a-1, b-1)$ mostra anche che $B \subseteq C$ è falsa, dato che appartiene a B ma non a C. □

Esercizio 4.19. Si consideri un predicato $P(x)$ dove la variabile x va scelta nell'insieme A. Definiamo l'*insieme di verità* $V(P(x))$ di $P(x)$ come il sottoinsieme di A costituito dagli elementi $a \in A$ tali che $P(a)$ è vera:

$$V(P(x)) = \{a \in A \mid P(a) \quad \text{è vera } \}$$

Tradurre con delle formule contenenti i quantificatori $\forall$ e $\exists$ le seguenti affermazioni a riguardo di $V(P(x))$:

- $V(P(x)) = \emptyset$
- $V(P(x)) \neq \emptyset$
- $V(P(x)) \neq A$
- $V(P(x)) = A$

Esercizio 4.20. Sia a un numero naturale e consideriamo i seguenti insiemi:

(1) $A = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x + y \geq 2a\}$
(2) $B = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \geq a \wedge y \geq a\}$
(3) $C = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x < a \to y \geq a\}$
(4) $D = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \geq a \to y < a\}$

(i) Ci sono inclusioni tra i quattro insiemi sopra elencati che valgono per ogni scelta di a?
(ii) Quali inclusioni sono certamente false per ogni scelta del parametro a?

Esercizio 4.21. Si trovino degli insiemi A, B, C di numeri naturali che verifichino entrambe le seguenti condizioni:

(1) $A \cap B \cap C^c$ ha tre elementi,
(2) $(A \cup B \cup C) \cap (A \cap B \cap C)^c$ ha dieci elementi.

Esercizio 4.22. Si consideri la seguente uguaglianza insiemistica:

$$(*) \quad (A \cap B) \times C = A \times (B \cap C)$$

(1) Stabilire se si possono scegliere gli insiemi A, B, C in modo che l'uguaglianza (*) sia vera.
(2) Stabilire se si possono scegliere gli insiemi A, B, C in modo che l'uguaglianza (*) sia falsa.
(3) Stabilire se (*) è sempre vera nel caso in cui $B \subseteq A$ e $C \subseteq A$.
(4) Stabilire se (*) è sempre vera nel caso in cui $A \cup C \subseteq B$.

Esercizio 4.23. Dati due insiemi A, B la loro differenza simmetrica $A\Delta B$ è definita da:

$$A\Delta B = (A \setminus B) \cup (B \setminus A).$$

(1) Dimostrare che $(A\Delta B)\Delta C = A\Delta(B\Delta C)$ (Quindi possiamo omettere le parentesi senza rischio di ambiguità).
(2) Semplificare le espressioni
   (i): $A \,\Delta\, A$,
   (ii): $A \,\Delta\, B \,\Delta\, A \,\Delta\, B \,\Delta\, B$,
   (iii): $A \,\Delta\, B \,\Delta\, A \,\Delta\, A \,\Delta\, B \,\Delta\, B$.
(3) Supponendo che $A = \{1, 2, 3\}$ e $B = \{2, 3, 4\}$, elencare gli elementi degli insiemi (i), (ii) e (iii) sopra definiti.

Esercizio 4.24. Si considerino i seguenti insiemi:

- $A = \{n \mid \exists k \in \mathbb{N} \quad k \leq 3 \ \wedge \ n = 3k\}$;
- $B = \{2n + 1 \mid n \in \mathbb{N} \ \wedge 1 \leq n \leq 5\}$;
- $C = \{(1, 2), (3, 4), (3, 3), (6, 7), (9, 9), (0, 3), (9, 7)\}$.

(1) Elenca gli elementi di A e di B ;
(2) Elenca gli elementi di $(A \times B) \cap (B \times A)$;
(3) Elenca gli elementi di $D = \{b \in B \mid \exists a \in A \ (a, b) \in C\}$.

Esercizio 4.25. Si considerino i seguenti sottoinsiemi di $\mathbb{N}$:

- $A = \{3, 4, 5, 6, 7, 8\}$;
- $B = \{4, 5, 6, 7, 9, 10, 11\}$;
- $C = \{1, 2, 3, 4, 5, 6, 10, 11\}$.

(1) Elenca gli elementi di

$$D = (A \cap B) \times (C \cap (B^c \cup (B \cap A)))$$

(l'operazione di complementare si intende rispetto all'insieme $\mathbb{N}$).
(2) Elenca gli elementi di

$$E = \{(x, y) \in D \mid x + y \leq 8\}$$

(3) Quante sono le funzioni

$$g : A \cap B \to C \cap (B^c \cup (B \cap A))$$

tali che l'insieme

$$G_g = \{(x, g(x)) \in (A \cap B) \times (C \cap (B^c \cup (B \cap A)))\}$$

è un sottoinsieme di E? (L'insieme G_g è il "grafico" della funzione g; questo concetto verrà discusso più estesamente nel Capitolo 6).

ESERCIZIO 4.26. Sia $D \subset \mathbb{Z}$ l'insieme dei numeri pari, $T \subset Z$ l'insieme dei numeri multipli di 3 e $C \subset Z$ l'insieme dei multipli di 5.

a) Costruire un insieme X tale che

$$D \cap T \cap C^c \subseteq X \subseteq (D \cup T \cup C) \cap (D \cap T \cap C)^c$$

b) Dire quanti sono gli insiemi X che soddisfano la condizione del punto a) e la ulteriore richiesta

$$X \subseteq \{1, 2, 3, \ldots, 100\}$$

ESERCIZIO 4.27. Sia $P = \mathcal{P}(\{1, 2, 3\})$ l'insieme delle parti di $\{1, 2, 3\}$.

(1) Elencare gli elementi di P e dire quanti sono.
(2) Stabilire se $\forall X, Y \in P\ (X \subseteq Y\ \vee\ Y \subseteq X)$.
(3) Stabilire se $\exists X, Y \in P\ (X \subseteq Y\ \vee\ Y \subseteq X)$.
(4) Stabilire se $\forall X \in P\ \exists Y \in P\ (X \cup Y = \{1, 2, 3\}\ \wedge\ X \cap Y = \emptyset)$.
(5) Stabilire se $\exists X \in P\ \forall Y \in P\ (X \cup Y = \{1, 2, 3\}\ \wedge\ X \cap Y = \emptyset)$.
(6) Stabilire se $\exists X \in P\ \forall Y \in P\ (X \cup Y = \{1, 2, 3\}\ \vee\ X \cap Y = \emptyset)$.

CAPITOLO 5

Induzione

1. Definizioni per induzione o "ricorsive"

Una successione di numeri è definita ricorsivamente se è data una regola che specifica il valore del termine iniziale e mostra come calcolarne un qualsiasi altro termine conoscendo il precedente. Un tipico esempio è la definizione della funzione fattoriale.

DEFINIZIONE 5.1. $0! = 1, (n+1)! = (n+1)n!$.

Prendendo $n = 4$ e applicando ripetutamente le regole otteniamo $4! = 4 \cdot 3! = 4 \cdot 3 \cdot 2! = 4 \cdot 3 \cdot 2 \cdot 1! = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0! = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = 4 \cdot 3 \cdot 2 \cdot 1 = 120$. Quindi il fattoriale $n!$ di un intero positivo n è il prodotto di tutti gli interi da 1 ad n.

In generale una definizione ricorsiva di una successione di numeri è data da una regola che specifica il valore del termine iniziale e mostra come calcolare il termine $n+1$-esimo a partire dal termine n-esimo.

Anche 2^n (il prodotto di n termini uguali a 2) può essere definito in maniera ricorsiva:

DEFINIZIONE 5.2. $2^0 = 1, 2^{n+1} = 2^n 2$.

Più in generale abbiamo:

DEFINIZIONE 5.3. Per ogni $x \in \mathbb{R}$, $x^0 = 1, x^{n+1} = x^n x$.

2. Dimostrazioni per induzione

Le dimostrazioni per induzione seguono un principio simile a quello delle definizioni ricorsive, con la differenza che in questo caso si tratta di uno strumento per *dimostrare* qualcosa anziché per *definire* qualcosa. Prima di enunciare il principio di induzione, illustriamolo con il seguente esempio.

ESEMPIO 5.4. Supponiamo di colorare i numeri interi con vari colori: verde, blu, giallo, rosso. Supponiamo si sapere che 4 è colorato di verde (Base dell'induzione) e che il successore di un numero verde è verde (Passo induttivo). Cosa possiamo concludere?

Un momento di riflessione ci porta inevitabilmente a:

SOLUZIONE: Tutti gli interi maggiori o uguali a 4 sono sicuramente verdi. Su quelli minori di 4 non abbiamo informazione: potrebbero essere verdi o di un altro colore. □

Vediamo ora come applicare lo stesso tipo di ragionamento per risolvere il seguente problema:

ESERCIZIO 5.5. Per quali n vale $n! > 2^n$?

SOLUZIONE: Coloriamo di verde gli n che verificano $n! > 2^n$ e di rosso tutti gli altri. Facili calcoli mostrano che $0, 1, 2, 3$ sono rossi ma 4 è verde. Chiediamoci cosa accade per i numeri maggiori di 4. A tal fine supponiamo che n sia un numero verde maggiore o uguale a 4, ovvero uno dei numeri ≥ 4 che verifica $2^n < n!$, e chiediamoci se il suo successore sia necessariamente verde, ovvero se $2^{n+1} < (n+1)!$. Quest'ultima è riscrivibile come

$2 \cdot 2^n < (n+1)n!$. Visto che $2 < (n+1)$ e che $2^n < n!$ (in quanto stiamo supponendo che n sia verde), il prodotto dei termini a sinistra è minore del prodotto dei termini a destra, ovvero $2 \cdot 2^n < (n+1)n!$, che è proprio quello che volevamo. Abbiamo quindi mostrato che il successore di un qualsiasi numero verde maggiore di 4 è verde, e visto che 4 stesso è verde, ne segue che tutti gli interi ≥ 4 sono verdi, cioè $\forall n \geq 4$ vale $n! > 2^n$. □

ESERCIZIO 5.6. Per quali $n \in \mathbb{N}$ vale $n^2 \leq 2^n$?

SOLUZIONE: Coloriamo di verde i numeri naturali n che verificano $n^2 \leq 2^n$ e di rosso tutti gli altri. Ad esempio facendo i calcoli si vede che $1, 2, 4, 5$ sono verdi, ma 3 è rosso. Visto che 4 è verde, se riuscissimo a dimostrare che il successore di un numero verde maggiore o uguale a 4 è verde, ne potremmo concludere che tutti gli interi n maggiori o uguali a 4 sono verdi. Per fare questa verifica supponiamo dunque che $n \geq 4$ sia un numero verde, ovvero uno dei numeri che verifica $n^2 \leq 2^n$, e cerchiamo di capire se il suo successore debba necessariamente essere verde, ovvero se $(n+1)^2 \leq 2^{n+1}$. Osserviamo che $(n+1)^2 = n^2 + 2n + 1 \leq 2^n + 2n + 1$, dove la disuguaglianza segue dal fatto che n era verde. Se riuscissimo a mostrare che

$$2^n + 2n + 1 \leq 2^{n+1} \qquad (*)$$

avremmo concluso componendo le disuguaglianze. Affrontiamo dunque la verifica di (*). Il termine destro 2^{n+1} si lascia riscrivere come $2 \cdot 2^n = 2^n + 2^n$, e cancellando un 2^n a sinistra e a destra la (*) diventa:

$$2n + 1 \leq 2^n. \qquad (**)$$

D'altra parte, siccome stiamo assumendo che n sia verde, abbiamo $n^2 \leq 2^n$, e pertanto per finire è sufficiente dimostrare che $2n + 1 \leq n^2$. Dividendo entrambi i membri per n, questa diventa $2 + 1/n \leq n$, che è sicuramente vera per $n \geq 4$ (anzi addirittura per $n \geq 3$) in quanto $1/n$ è minore di 1. Possiamo concludere che per ogni $n \geq 4$ vale $n^2 \leq 2^n$. □

Il principio di induzione (forma semplice).
Supponiamo che $P(n)$ sia un predicato che dipende da un numero intero $n \in \mathbb{Z}$. Se, dato un numero intero n_0, vale che:

- $P(n_0)$ è vera (*questa si chiama BASE dell'induzione*);
- per ogni intero $k \geq n_0$, è vera l'implicazione $P(k) \implies P(k+1)$ (*questo si chiama PASSO INDUTTIVO e la $P(k)$ si chiama IPOTESI INDUTTIVA*);

allora possiamo concludere che è vera la proposizione Q: "per ogni $n \geq n_0$, $P(n)$ è vera".

Espresso a parole, il passo induttivo dice che il successore di un numero $\geq n$ che gode della proprietà P gode anch'esso della proprietà P. La base dice che n gode della proprietà P. Si noti che n può anche essere negativo. Ad esempio se $n = -3$ la conclusione è che P vale sugli interi maggiori o uguali a -3.

Come potete notare, nell'enunciare il principio di induzione non abbiamo premesso la voce "Teorema", o "Proposizione". Per noi è come un assioma, ossia un fatto la cui validità sta alla base di tutti i nostri ragionamenti. In effetti il principio di induzione è legato all'esistenza dei numeri naturali, e lo accettiamo così come accettiamo i numeri naturali.

3. Somme parziali di successioni

Cominciamo con un breve richiamo sulle sommatorie.

DEFINIZIONE 5.7. Sommatorie: data una successione[1] di numeri $a_0, a_1, a_2, a_3, \ldots$ scriviamo $\Sigma_{i=m}^{n} a_i$ per indicare la somma di tutti i termini a_i della successione con i che varia tra m ed n (assumendo $m \leq n$). Ad esempio $\Sigma_{i=0}^{4} a_i = a_0 + a_1 + a_2 + a_3 + a_4$. Osserviamo che $\Sigma_{i=0}^{0} a_i = a_0$ e $\Sigma_{i=0}^{n+1} a_i = (\Sigma_{i=0}^{n} a_i) + a_{n+1}$. Quest'ultima uguaglianza dice che la somma di tutti i termini a_i per i che va da 0 ad $n+1$ si può spezzare nella somma degli a_i per i che va da 0 ad n a cui va poi sommato l'ultimo termine a_{n+1}.

La variabile i è "muta", nel senso che può essere sostituita con qualsiasi altra variabile non già utilizzata per altri scopi senza cambiare il significato dell'espressione. Ad esempio $\Sigma_{i=0}^{n} a_i$ può anche essere scritto come $\Sigma_{k=0}^{n} a_k$.

In questo paragrafo, studieremo alcune successioni "celebri" e troveremo delle formule per le somme dei primi n numeri della successione. Dimostreremo tali formule in vari modi (compresa l'induzione). Cominciamo dalla somma dei primi n numeri interi positivi.

ESERCIZIO 5.8. Dimostrare che, per ogni numero naturale positivo n vale:

$$\sum_{i=1}^{n} i = n(n+1)/2$$

SOLUZIONE: Proponiamo innanzitutto una "dimostrazione intuitiva". Consideriamo un rettangolo $n \times (n+1)$ (in Figura 1 troviamo il disegno nel caso 4×5). Una spezzata come quella in figura lo divide in due parti di area $\sum_{i=1}^{n} i$, dunque vale che $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

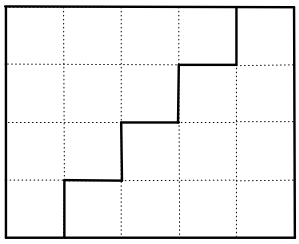

FIGURA 1. Un rettangolo 4×5 diviso in due parti ciascuna di area $1 + 2 + 3 + 4$.

Dimostriamo di nuovo la nostra formula, stavolta per induzione. Per prima cosa scegliamo il predicato $P(n)$. L'idea più semplice che viene in mente è quella giusta,e poniamo $P(n) =$"$\sum_{i=1}^{n} i = n(n+1)/2$".

La base dell'induzione in questo caso consiste nel verificare che $P(1)$ è vera e il passo induttivo consiste nel verificare che per ogni intero $k \geq 1$, è vera l'implicazione $P(k) \to P(k+1)$.

BASE. Questo non presenta difficoltà perché si verifica subito che $\sum_{i=1}^{1}$ è uguale a $\frac{1(1+1)}{2}$.

[1]Questo equivale a dire che, per ogni $i \in \mathbb{N}$, a_i è un numero intero. Sulle successioni torneremo in seguito con maggiori dettagli.

PASSO INDUTTIVO. Sia $k \geq 1$ un intero. Dobbiamo dimostrare che è vera l'implicazione:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2} \rightarrow \sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2}$$

Per far ciò basta dimostrare, che, se assumiamo vera la nostra ipotesi induttiva, ossia $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, allora deve essere vera $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2}$.

Procediamo; scriviamo $\sum_{i=1}^{k+1} i$ spezzando la somma così:

$$\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1)$$

Ma l'ipotesi induttiva ci permette di scrivere, al posto di $\left(\sum_{i=1}^{k} i\right)$, il suo valore $\frac{k(k+1)}{2}$. Dunque otteniamo

$$\sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + k + 1$$

che, riorganizzando il secondo membro, è proprio

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

come volevamo.

Il principio di induzione interviene a questo punto e ci permette di concludere che è vera la proposizione Q: "per ogni $n \in \mathbb{N} - \{0\}$, $P(n)$, ossia per ogni $n \in \mathbb{N} - \{0\}$ la somma dei primi n numeri naturali positivi è uguale a $\frac{n(n+1)}{2}$".

□

Esercizio 5.9. Dato un numero intero positivo n, la somma dei primi n numeri dispari è n^2.

Soluzione: Diamo tre dimostrazioni.

La prima è di natura intuitiva e si riferisce alla Figura 2. Un quadrato di lato n e di area n^2 può essere ottenuto sommando n "cornici" di area dispari, precisamente di area $1, 3, 5, \ldots, 2n-1$.

Proponiamo anche in questo caso una dimostrazione per induzione. Come predicato $P(n)$ scegliamo

$$P(n) : \sum_{i=0}^{n-1} (2i+1) = n^2$$

BASE. Si verifica subito che $P(1)$ è vera visto che si traduce nell'uguaglianza $1 = 1$.

PASSO INDUTTIVO. Sia $k \geq 1$ un intero. Dobbiamo dimostrare che è vera l'implicazione:

$$\sum_{i=0}^{k-1} (2i+1) = k^2 \rightarrow \sum_{i=0}^{k} (2i+1) = (k+1)^2$$

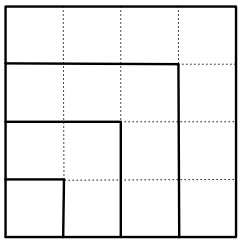

FIGURA 2. Il quadrato di lato 4 e area 4^2 si ottiene sommando "cornici" e quindi la sua area si può calcolare anche con la somma dei primi 4 numeri dispari: $1 + 3 + 5 + 7$.

Procediamo; scriviamo $\sum_{i=0}^{k}(2i+1)$ spezzando la somma così:

$$\sum_{i=0}^{k}(2i+1) = \left(\sum_{i=0}^{k-1}(2i+1)\right) + (2k+1)$$

Ma l'ipotesi induttiva ci permette di scrivere, al posto di $\left(\sum_{i=0}^{k-1}(2i+1)\right)$, il suo valore k^2. Dunque otteniamo

$$\sum_{i=0}^{k}(2i+1) = k^2 + 2k + 1$$

che, riorganizzando il secondo membro, è proprio

$$\sum_{i=0}^{k}(2i+1) = (k+1)^2$$

come volevamo.

Dimostriamo infine la formula ancora in un terzo modo. Possiamo esprimere la somma dei primi n numeri dispari con la sommatoria $\sum_{i=1}^{n}(2i-1)$. Alcuni passaggi algebrici ci permettono di scrivere:

$$\sum_{i=1}^{n}(2i-1) = 2\left(\sum_{i=1}^{n} i\right) + \sum_{i=1}^{n}(-1)$$

A questo punto conosciamo entrambe le sommatoria che compaiono nel membro di destra: la prima è uguale (vedi esercizio precedente) a $2(n(n+1)/2)$, la seconda a $-n$. Dunque abbiamo ottenuto che

$$\sum_{i=1}^{n}(2i-1) = n(n+1) - n = n^2$$

□

Generalizziamo:

ESEMPIO 5.10. Diremo che una successione di numeri reali $a_0, a_1, \ldots, a_n$ è una *progressione aritmetica* se le differenze $a_i - a_{i-1}$ sono tutte uguali fra loro (diciamo che siano tutte uguali al numero a). In generale una progressione aritmetica si può scrivere dicendo che, per ogni $i \in \mathbb{N}$, $a_i = ai + b$ per certi numeri reali fissati a e b.

Quanto vale $\sum_{i=0}^{n}(ai+b)$? Possiamo scrivere

$$\sum_{i=0}^{n}(ai+b) = a\left(\sum_{i=0}^{n} i\right) - \sum_{i=0}^{n} b = a(n(n+1)/2) - (n+1)b$$

Se in un problema capita di incontrare una sommatoria che non parte da 1 o da 0 ci si può sempre ricondurre, se conviene, al caso in cui parte da 1 o da 0. Ad esempio:

Esercizio 5.11. Calcolare la somma di tutti i numeri dispari compresi tra 100 a 1000.

Soluzione: Il primo dispari nell'intervallo è $101 = 2{\cdot}51-1$, l'ultimo è $999 = 2{\cdot}500-1$. Il valore cercato è $\sum_{i=51}^{500}(2i-1) = \sum_{i=1}^{500}(2i-1) - \sum_{i=1}^{50}(2i-1) = 500^2 - 50^2$. □

Occupiamoci ora di un altro tipo di successioni, le *progressioni geometriche*. Cominciamo con questo esercizio:

Esercizio 5.12. Dimostrare che, per ogni $n \in \mathbb{N}$,

$$\sum_{i=0}^{n} 1/2^i = 2 - 1/2^n$$

Soluzione: Possiamo procedere per induzione, scegliendo il predicato $P(n) : \sum_{i=0}^{n} 1/2^i = 2 - 1/2^n$. La base dell'induzione si riduce alla seguente verifica: $1 = 2 - 1/2^0$. Il passo induttivo richiede, assumendo vero $\sum_{i=0}^{n} 1/2^i = 2 - 1/2^n$, di dimostrare che $\sum_{i=0}^{n+1} 1/2^i = 2 - 1/2^{n+1}$. Possiamo scrivere:

$$\sum_{i=0}^{n+1} 1/2^i = \left(\sum_{i=0}^{n} 1/2^i\right) + 1/2^{n+1}$$

A questo punto, usando l'ipotesi induttiva, otteniamo

$$\sum_{i=0}^{n+1} 1/2^i = 2 - 1/2^n + 1/2^{n+1}$$

Visto che $-1/2^n + 1/2^{n+1} = -1/2^{n+1}$ abbiamo trovato l'uguaglianza desiderata[2]. □

Esempio 5.13. Diremo che una successione di numeri reali non nulli $b_0, b_1, \ldots, b_n$ è una *progressione geometrica* se i rapporti $\frac{b_i}{b_{i-1}}$ sono tutti uguali fra loro (diciamo che siano tutte uguali al numero k). In generale una progressione geometrica si può scrivere dicendo che, per ogni $i \in \mathbb{N}$, $b_i = ck^i$ per certi numeri reali non nulli fissati c e k.

Quanto vale $\sum_{i=0}^{n} ck^i$? Possiamo rispondere osservando che $\sum_{i=0}^{n} ck^i = c\sum_{i=0}^{n} k^i$. Se $k = 1$ allora la progressione geometrica è in realtà una successione costante, e la somma vale $ck(n+1)$. Se invece $k \neq 1$, possiamo partire calcolando

$$(1 + k + k^2 + \ldots + k^n)(k-1)$$

Svolgendo i calcoli si vede che molti termini si cancellano e rimane $k^{n+1} - 1$. Quindi vale:

$$1 + k + k^2 + \ldots + k^n = \frac{k^{n+1} - 1}{k - 1}$$

[2]La somma che abbiamo appena calcolato richiama il paradosso di Zenone di Elea (si tratta in realtà di una variante del celebre paradosso). Quando ci avviciniamo ad un oggetto possiamo osservare il nostro moto così: percorriamo metà della distanza che ci separa, poi metá della distanza rimanente, e così via... Lo raggiungeremo mai ? Vedi [] per qualche approfondimento

e possiamo concludere che

$$\sum_{i=0}^{n} ck^i = c\frac{k^{n+1}-1}{k-1}$$

4. Esercizi

ESERCIZIO 5.14. Determinare per quali numeri naturali n si ha $2^n > n^2 + 3n + 1$.

SOLUZIONE: Si comincia con dei tentativi e si scopre subito che la disuguaglianza non è vera per $n = 0, 1, 2, 3, 4, 5$, mentre è vera per $n = 6$ in quanto $2^6 = 64 > 6^2+3\cdot 6+1 = 55$. Proviamo allora per induzione che il predicato $T(n) : 2^n > n^2 + 3n + 1$ è vero per ogni $n \geq 6$. La base dell'induzione è stato già verificata. Dimostriamo allora il passo induttivo: fissiamo un intero k maggiore o uguale a 6 e proviamo che $T(k) \Rightarrow T(k + 1)$. In altre parole, prendendo per vero che (ipotesi induttiva):

$$2^k > k^2 + 3k + 1$$

dobbiamo dimostrare che:

$$2^{k+1} > (k + 1)^2 + 3(k + 1) + 1$$

Osserviamo che $2^{k+1} = 2 \cdot 2^k$ e allora, usando l'ipotesi induttiva possiamo scrivere:

$$2^{k+1} = 2 \cdot 2^k > 2(k^2 + 3k + 1)$$

A questo punto ci rendiamo conto che se è vera la disuguaglianza:

$$2(k^2 + 3k + 1) > (k + 1)^2 + 3(k + 1) + 1$$

abbiamo finito perché vale allora la catena di disuguaglianze:

$$2^{k+1} = 2 \cdot 2^k > 2(k^2 + 3k + 1) > (k + 1)^2 + 3(k + 1) + 1$$

Mostriamo dunque che

$$2(k^2 + 3k + 1) > (k + 1)^2 + 3(k + 1) + 1$$

Con qualche calcolo si nota che ciò equivale a

$$2k^2 + 6k + 2 > k^2 + 2k + 1 + 3k + 3 + 1 = k^2 + 5k + 5$$

che, semplificando ancora, diventa:

$$k^2 + k > 3$$

Visto che stiamo considerando i valori k maggiori o uguali a 6 questa ultima disuguaglianza è vera (se volete, potremmo concludere notando che, visto che $k \geq 6$, allora $k^2 + k \geq k \geq 6 > 3$). □

ESERCIZIO 5.15. Determinare per quali numeri naturali n si ha $n! > 2^n$.

SOLUZIONE: Verifichiamo subito che la disuguaglianza non è vera per $n = 0, 1, 2$ e 3, mentre è vera per $n = 4$ in quanto $4! = 24 > 16 = 2^4$. Proviamo allora per induzione che il predicato $P(n) : n! > 2^n$ è vero per ogni $n \geq 4$. La base dell'induzione $n = 4$ è stata appena verificata, dobbiamo quindi dimostrare il passo induttivo: fissiamo un intero k maggiore o uguale a 4 e proviamo che $P(k) \Rightarrow P(k + 1)$.

Infatti $(k+1)! = (k+1)\cdot k! > (k+1)2^k > 2\cdot 2^k = 2^{k+1}$, dove nella prima disuguaglianza abbiamo usato l'ipotesi induttiva, cioè $P(k)$ è vera, e nella seconda disuguaglianza usiamo $k + 1 > 2$, sicuramente vero per ogni $k \geq 4$ (in realtà basta $k \geq 1$). □

Esercizio 5.16. Trovare (e dimostrare rigorosamente che è valida) una formula per la somma dei primi n (con $n \geq 1$) numeri pari positivi.

Esercizio 5.17. Dimostrare che, per ogni $n \in \mathbb{N} - \{0\}$ vale:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Esercizio 5.18. Dimostrare che, per ogni $n \in \mathbb{N} - \{0\}$ vale:

$$\sum_{i=1}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2$$

Esercizio 5.19. Dimostrare per induzione la seguente formula per la somma dei cubi dei primi n numeri pari positivi:

$$\sum_{k=1}^{n} (2k)^3 = 2n^2(n+1)^2$$

Esercizio 5.20. Dimostrare che per ogni $n \geq 1$ si ha

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} \geq \sqrt{n}$$

Esercizio 5.21. Sia $H_k = \sum_{1=1}^{k} \frac{1}{i}$. Si dimostri che $H_{2^n} \geq 1 + \frac{n}{2}$.

Esercizio 5.22. Dimostrare che per ogni intero $n \geq 1$ vale:

$$\sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - \frac{1}{n}$$

Esercizio 5.23. Dimostrare che, per ogni n intero positivo, esistono almeno n numeri primi distinti che dividono il numero $2^{2^n} - 1$.[Suggerimento: $2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1)$.]

Esercizio 5.24. Consideriamo la formula

$$(1 - \frac{1}{4})(1 - \frac{1}{9})(1 - \frac{1}{16}) \cdots (1 - \frac{1}{n^2}) = \frac{an + b}{cn}$$

Proporre dei valori $a, b, c \in \mathbb{Z}$ per cui questa formula è vera per ogni $n \geq 2$ e dimostrare in tale caso la formula per induzione. La scelta di tali valori è unica ? Il numero $\frac{a}{c}$ è univocamente determinato ?

Esercizio 5.25. Dimostrare per induzione che per ogni intero $n \geq 14$ esistono interi non negativi $x, y \in \mathbb{N}$ tali che $n = 3x + 8y$.

Esercizio 5.26. Trovare, motivando la risposta, il più piccolo numero $n_0 \in \mathbb{N}$ tale che, per ogni $n \geq n_0$, valga

$$4^n \geq n^2 + 5n + 1$$

Esercizio 5.27.

a) Dati due numeri reali a, b compresi strettamente tra 0 e 1 si dimostri che

$$(1-a)(1-b) > 1 - a - b$$

b) Più in generale, dato $n \geq 2$ e dati n numeri reali $a_1, a_2, \ldots, a_n$ strettamente maggiori di zero e strettamente minori di uno, si dimostri per induzione che $(1-a_1)(1-a_2) \cdot \ldots \cdot (1-a_n) > 1 - a_1 - a_2 - \ldots - a_n$.

Esercizio 5.28 (Disuguaglianza di Bernoulli). Dimostrare che, per ogni $n \in \mathbb{N}$ e per ogni numero reale $x > -1$ vale

$$(1+x)^n \geq 1 + nx$$

Esercizio 5.29. Da un fagiolo magico germoglia una piantina alta un centimetro, che ogni giorno cresce di 1/30 della sua altezza. Dimostrare che dopo un anno la piantina avrà superato i 40 metri di altezza.

Esercizio 5.30. Togliamo una casella da una scacchiera di $2^n \times 2^n$ caselle. Dimostrare che è possibile ricoprire la parte rimanente con tessere tutte uguali fatte a L che ricoprono 3 caselle.

5. I numeri di Fibonacci e le successioni definite per ricorrenza.

Consideriamo la successione di numeri F_n ($n \in \mathbb{N}$) così definita:

- $F_0 = 0$
- $F_1 = 1$
- per ogni $n \geq 2$,

$$F_n = F_{n-1} + F_{n-2}$$

Per prima cosa "costruiamo" i primi numeri della successione :
$F_0 = 0$
$F_1 = 1$
$F_2 = F_0 + F_1 = 1$
$F_3 = F_2 + F_1 = 1 + 1 = 2$
$F_4 = 2 + 1 = 3$
$F_5 = 3 + 2 = 5$
$F_6 = 5 + 3 = 8$
$F_7 = 8 + 5 = 13$
$F_8 = 13 + 8 = 21$
e così via.. I numeri F_n si dicono **numeri di Fibonacci** (con riferimento a Leonardo

da Pisa, che pubblicò sotto il nome di Fibonacci il suo libro più celebre, *Liber abaci*, nel 1202)[3].

Osserviamo che, per conoscere il numero F_n non ci basta conoscere il numero precedente F_{n-1}, ma bisogna conoscere anche il numero F_{n-2}.

Una successione di questo tipo, ossia in cui il termine ennesimo si costruisce sapendo i termini precedenti, si dice *successione definita per ricorrenza*. Perché la successione sia ben definita, bisogna conoscere i valori iniziali. Per esempio, nel caso di Fibonacci, visto che ogni termine chiama in causa i due precedenti, F_0 e F_1 devono essere noti fin dall'inizio (non possono essere ricavati dalla "regola ricorsiva" $F_n = F_{n-1} + F_{n-2}$ che non li riguarda).

Un altro esempio di successione definita per ricorrenza potrebbe essere: $b_0 = 7$ e, per ogni $n \geq 1$, $b_n = 4b_{n-1}^2$.

6. Una formula per i numeri di Fibonacci

Partiamo da una successione, molto semplice, definita per ricorrenza:

$$a_0 = 1$$

$$a_n = 3a_{n-1} \qquad \forall n \geq 1$$

Sappiamo trovare una *formula* per a_n, ossia una equazione che ci permetta di calcolare a_n direttamente, senza dover calcolare prima a_{n-1}? Proviamo a scrivere i primi termini della successione:
$a_0 = 1$
$a_1 = 3 \cdot 1 = 3$
$a_2 = 3 \cdot 3 = 3^2$
$a_3 = 3 \cdot 3^2 = 3^3$
e così via.. Non ci mettiamo molto a congetturare che la formula giusta per a_n potrebbe essere:

$$a_n = 3^n$$

Dalla congettura alla dimostrazione in questo caso il passo è breve: ci basta notare che le due successioni $\{a_n\}$ e $\{3^n\}$ soddisfano la stessa regola ricorsiva e la stessa condizione iniziale, dunque si mostra facilmente per induzione che devono coincidere termine a termine, ossia $a_n = 3^n$ per ogni $n \in \mathbb{N}$.

Ma torniamo a Fibonacci: come possiamo trovare una formula per i numeri F_n ? Memori dell'esempio precedente, possiamo cominciare da un tentativo; proviamo se può funzionare una formula del tipo:

$$F_n = \alpha^n$$

per un qualche $\alpha \in \mathbb{R} - \{0\}$ (certamente $\alpha = 0$ non andrebbe bene, essendo $F_1 = 1$..).
Se fosse così, allora, visto che per $n \geq 3$ vale $F_n = F_{n-1} + F_{n-2}$, dovremmo avere

$$\alpha^n = \alpha^{n-1} + \alpha^{n-2}$$

che, dividendo per α^{n-2}, diventa

$$\alpha^2 = \alpha + 1$$

[3]Rispetto alla notazione usata a lezione, gli indici dei numeri F_n sono stati traslati di 1: a lezione avevo posto $F_0 = 1, F_1 = 1, F_2 = 2$ etc...

Più avanti, un'altra nota a pié di pagina vi inviterà a verificare che i risultati ottenuti qui e quelli ottenuti a lezione sono identici, a patto di tenere conto di questa traslazione di 1.

Quindi il nostro numero α dovrebbe essere una radice del polinomio $x^2 - x - 1$. Sappiamo che le radici di tale polinomio sono due:

$$\alpha = \frac{1+\sqrt{5}}{2} \qquad \beta = \frac{1-\sqrt{5}}{2}$$

Cominciamo a pensare di essere sulla strada giusta: infatti, rifacendo il ragionamento a ritroso, notiamo che con il nostro tentativo abbiamo trovato due numeri $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$ che soddisfano:

$$\alpha^2 = \alpha + 1 \qquad \beta^2 = \beta + 1$$

e quindi anche, per ogni $n \geq 2$:

$$\alpha^n = \alpha^{n-1} + \alpha^{n-2} \qquad \beta^n = \beta^{n-1} + \beta^{n-2}$$

Entrambe le successioni $\{\alpha^n\}$ e $\{\beta^n\}$ soddisfano dunque la stessa regola ricorsiva della successione di Fibonacci: per $n \geq 2$, il termine n-esimo è somma dei due termini precedenti.
Il problema è che né α^1 né β^1 sono uguali a F_1 che è 1. Inoltre α^0 e β^0 non sono uguali a F_0, che è 0.

In altre parole queste successioni non "partono" dagli stessi numeri con cui parte la successione di Fibonacci, dunque i loro termini sono poi molto diversi dai numeri di Fibonacci.

Possiamo rimediare però osservando che anche una successione del tipo $\{a\,\alpha^n + b\,\beta^n\}$, con a e b numeri reali qualunque, soddisfa la richiesta che il termine n-esimo sia somma dei due termini precedenti:

$$a\alpha^n + b\beta^n = (a\alpha^{n-1} + b\beta^{n-1}) + (a\alpha^{n-2} + b\beta^{n-2})$$

Dunque potremmo controllare se è possibile scegliere a e b in modo che $a\alpha^0 + b\beta^0 = 0$ e $a\alpha^1 + b\beta^1 = 1$. Si vede subito che il sistema di equazioni:

$$a\left(\frac{1+\sqrt{5}}{2}\right)^0 + b\left(\frac{1-\sqrt{5}}{2}\right)^0 = 0$$

$$a\left(\frac{1+\sqrt{5}}{2}\right)^1 + b\left(\frac{1-\sqrt{5}}{2}\right)^1 = 1$$

ha come unica soluzione $a = \dfrac{1}{\sqrt{5}}$, $b = -\dfrac{1}{\sqrt{5}}$. Dunque la successione $\{c_n\}$ definita, per ogni $n \in \mathbb{N}$, così:

$$c_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

soddisfa tutte le richieste della successione di Fibonacci.

Ripetiamo allora, per metterlo bene in evidenza, il ragionamento conclusivo: poiché entrambe le successioni soddisfano la stessa legge ricorsiva e le stesse condizioni iniziali, allora (si tratta di una facile applicazione del principio di induzione) coincidono, ossia $c_n = F_n$ per ogni $n \in \mathbb{N}$.

Abbiamo dunque dimostrato il seguente:

TEOREMA 5.31. *Dato $n \in \mathbb{N}$, vale la seguente formula per i numeri di Fibonacci*[4]*:*

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

7. Un metodo per le ricorrenze lineari a coefficienti costanti

Il metodo che abbiamo usato per trovare la formula per i numeri di Fibonacci è partito da un tentativo ("vediamo se per caso vanno bene soluzioni del tipo α^n") ma si è rivelato poi molto efficace. Osserviamo che, ripetendo il ragionamento, il metodo si può generalizzare al caso di successioni definite per ricorrenza in cui la legge ricorsiva sia *lineare e a coefficienti costanti*, ossia del tipo:

$$a_n = \gamma_1 a_{n-1} + \gamma_2 a_{n-2} + \gamma_3 a_{n-3} + \cdots + \gamma_i a_{n-i}$$

dove i γ_j sono numeri complessi.
Per esempio prendiamo, per $n \geq 4$, la legge

$$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$$

con le condizioni iniziali

$$a_1 = 4 \quad a_2 = 22 \quad a_3 = 82$$

Lo stesso ragionamento usato per Fibonacci ci porta a cercare le radici del polinomio $x^3 - 6x^2 + 11x - 6$. Tali radici (che in generale possiamo cercare in $\mathbb{C}$) si trovano in questo caso molto facilmente e sono 1, 2 e 3; allora tutte le successioni del tipo

$$a\ 1^n + b\ 2^n + c\ 3^n$$

con a, b, c numeri reali qualsiasi soddisfano la legge ricorsiva data. Facendo il sistema di tre equazioni per imporre che valgano le 3 condizioni iniziali si trova che la formula per la successione a_n è, per ogni $n \geq 1$:

$$a_n = -2 \cdot 1^n + (-3) \cdot\ 2^n + 4 \cdot\ 3^n$$

Quindi quando avete di fronte una successione definita per ricorrenza lineare e a coefficienti costanti potete tentare di applicare questo metodo per trovare la formula per il termine ennesimo.
Vi avvertiamo però che, quando cercate le radici del polinomio, possono capitare situazioni che richiedono ulteriori approfondimenti. Per esempio studiamo il caso di una successione che soddisfa, per $n \geq 2$, la legge

$$b_n = 4b_{n-1} - 4b_{n-2}$$

con le condizioni iniziali

$$b_0 = 5 \quad b_1 = 7$$

Il polinomio associato è $x^2 - 4x + 4$ che è $(x-2)^2$ ossia ha come radice 2 "ripetuta due volte" (detto meglio: con molteplicità due). Questo è dunque un caso che prima non avevamo trattato: qui le successioni che si usano sono $\{2^n\}$ e la sua "derivata" $\{n2^{n-1}\}$. Le successioni del tipo

$$a\ 2^n + b\ n2^{n-1}$$

[4]Potete verificare che anche la formula data a lezione forniva i "numeri giusti", ovviamente con la traslazione di 1 dell'indice.

con a, b numeri reali qualsiasi soddisfano tutte la legge ricorsiva data. Facendo il sistema di due equazioni per imporre che valgano le due condizioni iniziali si trova che la formula per la successione b_n è, per ogni $n \geq 0$:

$$b_n = 5 \cdot \ 2^n - 3 \cdot \ n2^{n-1}$$

Certamente, durante l'applicazione di questo metodo, può sorgere una difficoltà, ossia può risultare molto difficile trovare le radici in $\mathbb{C}$ del polinomio associato alla successione. A questo non c'è rimedio, visto che in generale il problema di trovare radici di polinomi è molto difficile; possiamo però garantirvi che negli esercizi che vi proporremo di svolgere in questo corso i polinomi saranno sempre "alla portata".

Per quello che riguarda il sistema finale che mette in gioco le condizioni iniziali, c'è una buona notizia, perché, come imparerete nel corso di Geometria 1, quel tipo di sistemi ha sempre una unica soluzione (la matrice che descrive il sistema è una *matrice di Vandermonde*).

Suggerimento per una ricerca. Il numero $\alpha = \frac{1+\sqrt{5}}{2}$ è il cosiddetto "rapporto aureo", ossia il rapporto fra la lunghezza di un segmento e quella della sua "sezione aurea". Sapete cosa è ?

8. Forme equivalenti del principio di induzione: il principio del minimo e il principio di induzione forte

Ci sono altri due modi con cui si può enunciare il principio di induzione: l'assioma del buon ordinamento (detto anche "principio del minimo") e il principio di induzione "forte". Anche se a prima vista non sembrerebbe, si può in realtà dimostrare che il principio di induzione, il principio di induzione forte e l'assioma del buon ordinamento sono equivalenti. Come conseguenza pratica, questo vuol dire che se un problema si può risolvere usando uno di questi tre assiomi, allora c'è sicuramente il modo di risolverlo anche usando uno qualunque degli altri due.

Il principio di induzione forte.
Supponiamo che $P(n)$ sia un predicato che dipende da un numero naturale $n \in \mathbb{N}$. Se, dato un numero naturale n_0, vale che:

- $P(n_0)$ è vera (*questa si chiama BASE dell'induzione*);
- per ogni intero $k \geq n_0$, è vera l'implicazione

$$(P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)) \to P(k+1)$$

(*questo si chiama PASSO INDUTTIVO e la* $P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)$ *si chiama IPOTESI INDUTTIVA*);

allora possiamo concludere che è vera la proposizione Q: "per ogni $n \geq n_0$, $P(n)$ è vera".

Osserviamo che, in questo caso, la base dell'induzione è la stessa del "normale" principio di induzione, ma il passo induttivo è diverso. Nell'induzione normale, si deve dimostrare che, per ogni intero $k \geq n_0$, è vera l'implicazione $P(k) \to P(k+1)$. Questo si traduce nel tentativo di dimostrare $P(k+1)$ assumendo come vera la $P(k)$. Dunque, nel momento in cui dimostriamo la $P(k+1)$, abbiamo un'arma a nostro vantaggio, ossia la $P(k)$.

Nell'induzione forte, invece, il passo induttivo chiede di dimostrare che, per ogni intero $k \geq n_0$, è vera l'implicazione

$$(P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)) \rightarrow P(k+1)$$

Questo si traduce come prima nel tentativo di dimostrare la $P(k+1)$, ma stavolta si possono assumere come vere tutte le proposizioni $P(n_0), P(n_0+1), \ldots, P(k)$; dunque nel momento in cui dimostriamo la $P(k+1)$ siamo più "forti" (ecco perché si chiama induzione "forte"), perché abbiamo a nostro vantaggio molte armi, non solo la $P(k)$, che avevamo anche nell'induzione normale, ma anche le altre proposizioni $P(n_0), P(n_0+1), \ldots, P(k-1)$ (*ricordatevi però che siamo più forti solo apparentemente, perché in realtà l'induzione forte è equivalente all'induzione semplice*).

Esempio 5.32. Dimostrare usando l'induzione forte che ogni numero intero ≥ 2 o è primo o si può scrivere come prodotto di numeri primi [5].

La proposizione che vogliamo provare per induzione forte è Q : "per ogni $n \geq 2$ il numero n o è primo o si può scrivere come prodotto di numeri primi".
Consideriamo dunque il predicato $P(n)$:"il numero n o è primo o si può scrivere come prodotto di numeri primi".

La base, ossia la dimostrazione di $P(2)$, è immediata, perché 2 è appunto un numero primo.
Adesso occupiamoci del passo induttivo. Supponiamo (induzione forte !) che siano vere tutte le proposizioni $P(j)$ con $2 \leq j \leq k$ e cerchiamo di dimostrare che è vera $P(k+1)$, ossia dobbiamo dimostrare che: "il numero $k+1$ o è primo o si può scrivere come prodotto di numeri primi".

Ora si possono verificare due casi: o $k+1$ è primo, e in tal caso la dimostrazione del passo induttivo è già finita, oppure $k+1$ non è primo. In questo secondo caso, allora $k+1$ è composto e si potrà scrivere come prodotto di due numeri a e b, $k+1 = ab$, dove $1 < a < k+1$ e $1 < b < k+1$. Quindi a e b sono tali che le proposizioni $P(a)$ e $P(b)$ risultano vere per ipotesi induttiva, garantendoci che a e b o sono primi o si possono scrivere come prodotto di numeri primi. Di conseguenza $k+1 = ab$ si scrive come prodotto di numeri primi (quelli della decomposizione di a per quelli della decomposizione di $b \ldots$).

Osservazione 5.33. Per dimostrare questa stessa proposizione usando l'induzione semplice, basta cambiare il predicato, quello giusto è $T(n)$:"ogni numero intero maggiore o uguale a 2 e minore o uguale a n è o primo o prodotto di primi". Provate a completare la dimostrazione, che è simile alla precedente .....

Quando, nel Capitolo 5 abbiamo introdotto il principio di induzione abbiamo detto che è legato alla esistenza dei numeri naturali. Questo viene messo particolarmente in luce se enunciamo il principio di induzione in questa forma:

Assioma del buon ordinamento (chiamato anche "Principio del minimo").
Ogni sottoinsieme NON VUOTO di $\mathbb{N}$ ha un elemento minimo.

Vedremo più avanti in questo corso alcune dimostrazioni in cui risulta naturale applicare l'induzione nella forma data dall'assioma del buon ordinamento. Per il momento

[5]Chi vuole rivedere la definizione di numero primo può consultare più avanti il Capitolo **??**.

torniamo all'esempio precedente e vediamo come il principio del minimo possa essere usato per dare una variante della dimostrazione.

ESEMPIO 5.34. Dimostrare usando il principio del minimo che ogni numero intero ≥ 2 o è primo o si può scrivere come prodotto di numeri primi.

Consideriamo il predicato $P(n)$: "il numero n o è primo o si può scrivere come prodotto di numeri primi" e sia S l'insieme dei numeri interi $m \geq 2$ tali che la proposizione $P(m)$ è falsa.

Osserviamo che dimostrare l'enunciato equivale a dimostrare che S è vuoto. Procediamo per assurdo e supponiamo dunque per assurdo che S non sia vuoto. Allora S, che è un sottoinsieme non vuoto di $\mathbb{N}$, per il principio del minimo ha un elemento minimo, che chiamiamo s.

Riassumendo, cosa sappiamo di s ? Sappiamo che è un intero ≥ 2 tale che $P(s)$ è falsa, ossia che non è né primo né prodotto di primi, e che è il più piccolo numero con queste caratteristiche.

In particolare, non essendo primo si potrà scrivere come prodotto di due numeri a e b, $s = ab$, dove $1 < a < s$ e $1 < b < s$. Quindi a e b, essendo ≥ 2 e strettamente minori di s sono tali che le proposizioni $P(a)$ e $P(b)$ sono vere (altrimenti sarebbe uno di loro, e non s, il minimo dell'insieme S..). Questo vuol dire che a e b sono o primi o prodotto di primi e ci permette di ottenere una decomposizione in primi di s. Abbiamo ottenuto un assurdo, perché s per costruzione non può ammettere una decomposizione in primi.

Siccome aver assunto che S sia diverso dall'insieme vuoto ci ha portati ad un assurdo, abbiamo dunque dimostrato che $S = \emptyset$ come volevamo.

9. Esercizi

ESERCIZIO 5.35. Sia $\{u_n\}_{n\in\mathbb{N}}$ la successione così definita:

$$\begin{aligned} u_0 &= 0 \\ u_{k+1} &= 3u_k + 3^k \end{aligned}$$

Dimostrare che $u_k = k3^{k-1}\ \forall\ k \in \mathbb{N}$. [Osservazione: la successione proposta non è "lineare a coefficienti costanti" dunque non si applica il metodo descritto nei paragrafi precedenti]

ESERCIZIO 5.36. Definiamo per ricorrenza $a_0 = 0, a_1 = 12$ e $a_{n+2} = 6a_{n+1} - 9a_n$. Trovare una formula per a_n.

ESERCIZIO 5.37. Consideriamo la successione definita per ricorrenza da $a_0 = 8, a_1 = -1$ e, per ogni numero intero $n \geq 2$, dalla regola:

$$a_n = -a_{n-1} + 2a_{n-2}$$

Trovare un formula per a_n.

ESERCIZIO 5.38. Si definisca una successione tramite la regola $a_0 = 2, a_1 = 1$ e, per ogni $n \geq 1$, $a_{n+1} = a_n + 6a_{n-1}$. Si trovi una formula per il termine a_n.

ESERCIZIO 5.39. Si consideri la successione data da $a_0 = 1$ e $a_{n+1} = 2a_n + 3$.
a) Si dimostri che, per ogni $n \geq 1$, $2^n \mid a_n + 3$.
b) Si trovi una formula per a_n. [Osservazione: la successione proposta non è lineare.]

ESERCIZIO 5.40. Si consideri la successione data da $a_0 = 1$, $a_1 = 1$ e $a_n = a_{n-2} + n$.
a) Trovare, motivando la risposta, il più piccolo numero $n_0 \in \mathbb{N}$ tale che, per ogni $n \geq n_0$,

vale $a_n \geq 2n$.
b) Trovare una formula per a_n.

Esercizio 5.41. Sia a_n una successione di numeri interi tale che $a_0 = 1$, $a_{n+1} \geq 2a_n$ se n è pari, e $a_{n+1} \geq 3a_n$ se n è dispari. Dimostrare che per ogni $n \in \mathbb{N}$, $a_{2n} \geq 6^n$.

Esercizio 5.42. Questo problema è ricavato dal *Liber Abaci* (del 1202..) di Fibonacci. "Un uomo mise una coppia di conigli in un luogo circondato da tutti i lati da un muro. Quante coppie di conigli possono essere prodotte dalla coppia iniziale in un anno, supponendo che ogni mese ogni coppia produca una nuova coppia in grado di riprodursi a sua volta dal secondo mese?"

Esercizio 5.43. Dato $n \in \mathbb{N} - \{0\}$, sia S_n il numero di tutte le possibili stringhe (cioè liste ordinate) di cifre binarie (ossia 0 e 1) che hanno le seguenti caratteristiche:

- hanno lunghezza n
- se $n = 1$ la stringa è 0, se $n \geq 2$ la lista comincia per 01
- non ci sono mai tre cifre uguali consecutive

Per esempio $S_5 = 5$ e le stringhe in questione sono 01001, 01010, 01011, 01100, 01101. Dimostrare che, per ogni $n \in \mathbb{N} - \{0\}$, $S_n = F_n$.

Esercizio 5.44. Una lista di numeri interi strettamente crescente si dice *di parità alterna* se inizia con un numero dispari, ha come secondo termine un numero pari, poi il terzo termine è dispari, il quarto è pari, e così via. La lista vuota viene considerata anch'essa una lista di parità alterna. Sia $P(n)$ il numero delle liste di parità alterna i cui termini costituiscono un sottoinsieme di $\{1, 2, \ldots, n\}$. Che relazione c'è fra le successioni $\{P_n\}$ e $\{F_n\}$?

Esercizio 5.45. Provare che per i numeri di Fibonacci F_n ($n \geq 0$) vale la seguente formula:

$$F_{n+4} = F_3 F_n + F_4 F_{n+1}$$

Esercizio 5.46. Provare che per i numeri di Fibonacci F_n vale la seguente formula ($n \geq 0$ e $m \geq 1$):

$$F_{n+m} = F_{m-1} F_n + F_m F_{n+1}$$

Esercizio 5.47. Provare che per i numeri di Fibonacci si ha che F_n divide F_{mn} ($n \geq 1$, $m \geq 0$).

Esercizio 5.48. Provare che per i numeri di Fibonacci si ha che $F_{n+4} \geq n^2$ per $n \geq 0$.

Esercizio 5.49. Data la successione $\{a_n\}$ definita da $a_0 = 1$,

$$a_n = 1 + a_0 + a_1 + \cdots + a_{n-1} \qquad \forall n \geq 1$$

trovare una formula per a_n.

Trovare una formula per la successione $\{b_n\}$ definita da $b_0 = 1$,

$$b_n = 1 - b_0 + b_1 - b_2 + \cdots + (-1)^n b_{n-1} \qquad \forall n \geq 1$$

[Osservazione: le successioni proposte non sono lineari.]

Esercizio 5.50. Sia $\{u_n\}_{n \in \mathbb{N}}$ la successione così definita:

$$\begin{aligned} u_0 &= 0 \\ u_{k+1} &= 3u_k + 3^k \end{aligned}$$

Dimostrare che $u_k = k3^{k-1}$ $\forall$ $k \in \mathbb{N}$.

SOLUZIONE: Base: $u_0 = 0 = 0 \cdot 3^{-1}$.

Passo Induttivo: suppongo che, per un $k \geq 0$, sia vero $u_k = k3^{k-1}$ (ipotesi induttiva) e voglio dimostrare $u_{k+1} = (k+1)3^k$. Ma $u_{k+1} = 3u_k + 3^k$ per come è definita la successione. Ora, utilizzando l'ipotesi induttiva posso scrivere che

$$3u_k + 3^k = 3(k3^{k-1}) + 3^k = k3^k + 3^k = (k+1)3^k$$

In conclusione ho trovato $u_{k+1} = (k+1)3^k$ come volevo. Il principio di induzione garantisce allora che $u_k = k3^{k-1}\ \forall\ k \in \mathbb{N}$. □

ESERCIZIO 5.51. Sia $\{(a_n, b_n)\}_{n\geq 0}$ una successione di elementi di $\mathbb{Z} \times \mathbb{Z}$ definita da

$$\begin{cases} (a_0, b_0) = (1, -1), \\ (a_{n+1}, b_{n+1}) = (a_n + b_n, a_n - b_n) \text{ per } n \text{ maggiore o uguale a } 0. \end{cases}$$

Dimostrare che per ogni $n \geq 0$ si ha:

(i) la somma $a_n + b_n$ è un numero pari,
(ii) $(a_{2n}, b_{2n}) = (2^n, -2^n)$,
(iii) $(a_{2n+1}, b_{2n+1}) = (0, 2^{n+1})$.

SOLUZIONE:

(i) Per $n = 0$ abbiamo $a_0 + b_0 = 1 - 1 = 0$ che è un numero pari. Inoltre per ogni intero naturale n abbiamo $a_{n+1} + b_{n+1} = (a_n + b_n) + (a_n - b_n) = 2a_n$; ciò prova che $a_{n+1} + b_{n+1}$ è un numero pari.

(ii) Osserviamo che per $n \geq 1$, usando due volte la definizione induttiva della successione, abbiamo

$$\begin{aligned} (a_{2(n+1)}, b_{2(n+1)}) &= (a_{2n+1} + b_{2n+1}, a_{2n+1} - b_{2n+1}) \\ &= (a_{2n} + b_{2n} + a_{2n} - b_{2n}, a_{2n} + b_{2n} - a_{2n} + b_{2n}) \\ &= (2a_{2n}, 2b_{2n}). \end{aligned}$$

Possiamo ora facilmente dimostrare per induzione che il predicato $p(n) : (a_{2n}, b_{2n}) = (2^n, -2^n)$ è vero per ogni intero naturale $n \geq 0$. Per quel che riguarda la base dell'induzione abbiamo $(a_0, b_0) = (1, -1) = (2^0, -2^0)$ dalla definizione e quindi $p(0)$ è vera.

Vediamo ora il passo induttivo. Supponiamo quindi vera $p(k)$ e dimostriamo che anche $p(k+1)$ è vera. Per quanto visto sopra abbiamo $(a_{2(k+1)}, b_{2(k+1)}) = (2a_{2k}, 2b_{2k}) = (2 \cdot 2^k, -2 \cdot 2^k) = (2^{k+1}, -2^{k+1})$. La proposizione $\forall n \geq p(n)$ è quindi provata.

(iii) Usando quanto appena dimostrato nel punto precedente e la definizione induttiva della successione abbiamo: $(a_{2n+1}, b_{2n+1}) = (a_{2n} + b_{2n}, a_{2n} - b_{2n}) = (2^n - 2^n, 2^n + 2^n) = (0, 2^{n+1})$. E quindi quanto richiesto è provato.

□

ESERCIZIO 5.52. Sia a_n una successione di numeri interi tale che $a_0 = 1$, $a_{n+1} \geq 2a_n$ se n è pari, e $a_{n+1} \geq 3a_n$ se n è dispari. Dimostrare che per ogni $n \in \mathbb{N}$, $a_{2n} \geq 6^n$.

ESERCIZIO 5.53. Fate finta di non aver letto la dimostrazione contenuta in questo capitolo e poniamo che vi venga proposta, facendola "cadere dal cielo", la formula per i numeri di Fibonacci:

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

Dimostratela usando l'induzione forte.

Esercizio 5.54. Si definisca una successione tramite la regola $a_0 = 2, a_1 = 1$ e, per ogni $n \geq 1$, $a_{n+1} = a_n + 6a_{n-1}$. Si dimostri che, per ogni $n \in \mathbb{N}$,

$$a_n \geq 3^{n-1}$$

Si trovi una formula per il termine generale a_n.

Esercizio 5.55. Consideriamo la successione definita per ricorrenza da $a_0 = 8, a_1 = -1$ e, per ogni numero intero $n \geq 2$, dalla regola:

$$a_n = -a_{n-1} + 2a_{n-2}$$

a) Scrivere i primi 4 termini della successione.
b) Dimostrare che se n è pari allora a_n è positivo, se n è dispari allora a_n è negativo.
c) Determinare se esistono degli interi a, b tali che per ogni $n \in \mathbb{N}$:

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

Esercizio 5.56. Dato un poligono convesso con n lati, determinare il massimo numero di diagonali che è possibile tracciare da un vertice a un altro del poligono in modo che due di tali diagonali non si intersechino mai al di fuori dei vertici.

CAPITOLO 6

Prodotto cartesiano, relazioni e funzioni

1. Le definizione di funzione

Consideriamo due insiemi X e Y.

DEFINIZIONE 6.1. Una funzione f da X a Y assegna ad ogni elemento x di X uno ed un solo elemento $f(x)$ di Y. Dato $x \in X$, l'elemento $y = f(x) \in Y$ è l'"immagine" di x tramite f, mentre, dato $y \in Y$, un elemento $z \in X$ tale che $f(z) = y$ è una "controimmagine" di y (ce ne può essere una, più di una, o nessuna). Si scrive

$$f : X \to Y$$

per indicare il fatto che f è una funzione da X ad Y. L'insieme X si chiama "dominio" della funzione e l'insieme Y "codominio" della funzione. L'immagine Imm f della funzione è il sottoinsieme di Y costituito dalle immagini degli elementi di X tramite la funzione, ossia:

$$\text{Imm } f = \{y \in Y \mid \exists x \in X \quad f(x) = y\}.$$

Per indicare l'immagine di f si una anche la notazione

$$\text{Imm } f = \{f(x) \mid x \in X\}$$

Osserviamo che l'immagine di f è il sottoinsieme degli elementi di Y che hanno almeno una controimmagine.

Rimarchiamo che una funzione è specificata da una **terna** di informazioni: il dominio, il codominio e la legge che spiega come assegnare ad ogni elemento del dominio la sua immagine. Due funzioni f e g sono uguali se e solo se hanno lo stesso dominio, lo stesso codominio e per ogni x nel comune dominio si ha $f(x) = g(x)$.

2. Primi esempi

ESEMPIO 6.2. Consideriamo le seguenti funzioni:

$$f : \mathbb{R} \to \mathbb{R} \qquad f(x) = x^4$$

$$g : \mathbb{R}^{\geq 0} \to \mathbb{R} \qquad g(x) = x^4$$

$$h : \mathbb{R} \to \mathbb{R}^{\geq 0} \qquad h(x) = x^4$$

$$\phi : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0} \qquad \phi(x) = x^4$$

Si tratta di funzioni tutte diverse fra loro, anche se la legge è la stessa (ossia elevare alla quarta il numero x); si differenziano l'una dall'altra perché cambiano il dominio e/o il codominio.
Quando si vuole costruire una funzione, bisogna sempre prestare molta attenzione a che sia ben definita, ossia che soddisfi tutte le richieste della Definizione 6.1.

Esempio 6.3. Ecco un tentativo di costruire una funzione:

$$f : \mathbb{R} \to \mathbb{R} \qquad f(x) = \frac{1}{x}$$

Questa **non** è una buona definizione. Infatti quanto abbiamo scritto non dice quale è l'immagine dell'elemento 0 che appartiene al dominio ($\frac{1}{0}$ non è definito).

Le funzioni f_1 e f_2 seguenti sono invece ben definite:

$$f_1 : \mathbb{R} - \{0\} \quad \to \quad \mathbb{R} \qquad f(x) = \frac{1}{x}$$

$$f_2 : \mathbb{R} \to \mathbb{R} \qquad f(x) = \frac{1}{x} \text{ se } x \neq 0 \text{ e } f(0) = 42$$

Esempio 6.4. Può capitare che stessa funzione venga descritta in più modi apparentemente diversi. Ecco tre diverse presentazioni della stessa funzione. Siano $X = \{1, 2, 5, 30, 1000\}$ e $Y = \{1, 4, 25, 26, 900, 950, 999, 1000000, 10101010\}$.
Prima presentazione:

$f : X \to Y$ $\qquad$ $f(x)$ è il più piccolo elemento di Y che è maggiore o uguale a x

Seconda presentazione:

$$f : X \to Y \qquad f(x) = x^2$$

Terza presentazione:

$$f : X \to Y \qquad f(1) = 1, f(2) = 4, f(5) = 25, f(30) = 900, f(1000) = 1000000$$

L'ultima presentazione di f specifica esplicitamente una per una le immagini degli elementi di X. Una simile descrizione si può utilizzare quando il dominio è un insieme finito (e gli elementi non sono troppi....).

3. Funzioni iniettive, surgettive, bigettive

Definizione 6.5 (Funzione iniettiva). Consideriamo una funzione $f : X \to Y$.

Se per ogni elemento $y \in Y$ vale che y ha al più una controimmagine (cioè ne ha zero o una sola), la funzione si dice *iniettiva*. Questo si può esprimere anche scrivendo la seguente proposizione a riguardo della f:

$$\forall x_1, x_2 \in X \quad x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

o, in modo equivalente, utilizzando la contronominale dell'implicazione:

$$\forall x_1, x_2 \in X \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

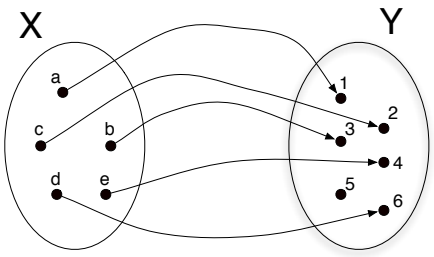

Figura 1. Una funzione iniettiva: non c'è nessun elemento di Y su cui arrivano due frecce.

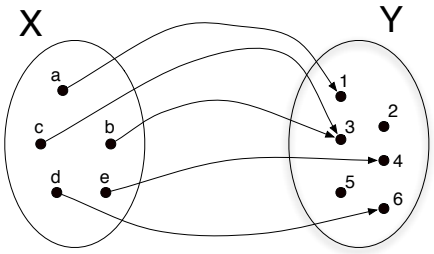

FIGURA 2. Una funzione NON iniettiva: infatti gli elementi b e c di X hanno la stessa immagine.

DEFINIZIONE 6.6 (Funzione surgettiva). Consideriamo una funzione $f : X \to Y$.

Se ogni elemento $y \in Y$ ha almeno una controimmagine, la funzione si dice *surgettiva*. Questo si può esprimere anche scrivendo la seguente proposizione:

$$\forall y \in Y \quad \exists x \in X \quad f(x) = y$$

oppure, in maniera equivalente, coinvolgendo l'insieme Imm f:

$$\text{Imm } f = Y$$

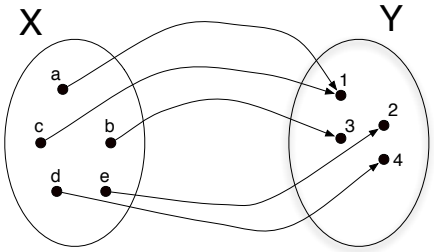

FIGURA 3. Una funzione surgettiva: su ogni elemento di Y arriva almeno una freccia. La funzione non è iniettiva.

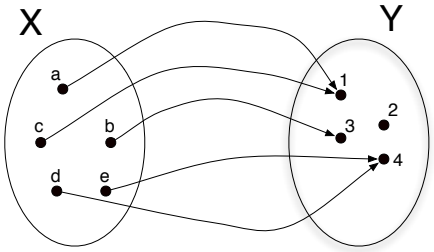

FIGURA 4. Una funzione NON surgettiva: infatti l'elemento $2 \in Y$ non è immagine di alcun elemento di X. La funzione non è iniettiva.

DEFINIZIONE 6.7 (Funzione bigettiva). Consideriamo una funzione $f : X \to Y$.

Se f è sia iniettiva sia surgettiva allora si dice *bigettiva*. Questo si può esprimere anche dicendo che ogni elemento $y \in Y$ ha esattamente una controimmagine, o scrivendo la seguente proposizione:

$$(\forall x_1, x_2 \in X \quad x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)) \ \wedge \ (\forall y \in Y \quad \exists x \in X \quad f(x) = y)$$

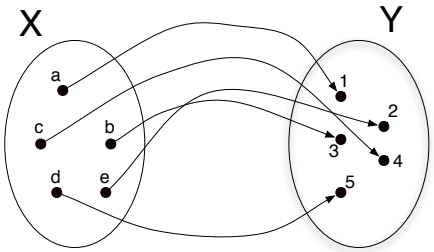

FIGURA 5. Una funzione bigettiva: su ogni elemento di Y arriva una ed una sola freccia. Osserviamo che X e Y hanno lo stesso numero di elementi.

4. Provare a scoprire se una funzione è iniettiva, surgettiva, bigettiva...esempi

Come primo esercizio, potete studiare le quattro funzioni f, g, h, ϕ descritte nell'Esempio 6.2 del paragrafo precedente: f non è né surgettiva né iniettiva, g è iniettiva ma non surgettiva, h è surgettiva ma non iniettiva e ϕ è bigettiva.

Sia $X = Y = \{1, 2, 3, 4\}$ e consideriamo la funzione:

$$f \ : \ \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$$

tale che $f(1) = 1$ $f(2) = 1$ $f(3) = 4$ $f(4) = 3$. Questa funzione non è né iniettiva né surgettiva (e dunque neppure bigettiva). Non è iniettiva perché ci sono due elementi del dominio (i numeri 1 e 2) che hanno la stessa immagine e non è surgettiva perché c'è un elemento del codominio (il numero 2) che non appartiene a Imm f.

Consideriamo adesso la funzione $g \ : \ \mathbb{N} \to \mathbb{N}$ tale che $g(n) = 2n$ per ogni numero $n \in \mathbb{N}$. Questa funzione è iniettiva; per dimostrarlo possiamo per esempio verificare che, se accade che $g(n) = g(m)$, allora $n = m$. Questa verifica è immediata: infatti $g(n) = g(m)$ significa $2n = 2m$ da cui, dividendo per 2, si ricava subito $n = m$. La funzione invece non è surgettiva (e dunque non è bigettiva) perché Imm f è il sottoinsieme di $\mathbb{N}$ costituito dai numeri pari e quindi non coincide con tutto il codominio $\mathbb{N}$.

Studiamo la funzione $h \ : \ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definita da $h(n, m) = 2n + 3m$, dove $(n, m) \in \mathbb{N} \times \mathbb{N}$. Si osserva subito che non è iniettiva (infatti $h(3, 0) = h(0, 2)$). Inoltre è surgettiva. Infatti ogni numero intero appartiene a Imm h: se considero un numero pari, diciamo $2k$, lo posso ottenere per esempio come immagine della coppia $(k, 0)$; se considero un numero dispari, diciamo $2l + 1$, lo posso ottenere come immagine della coppia $(l - 1, 1)$.

Domanda in più: dato un elemento in $y \in \mathbb{N}$, quante sono le sue controimmagini, ossia gli elementi (n, m) di $\mathbb{N} \times \mathbb{N}$ tali che $h(n, m) = y$?...

Consideriamo infine la funzione θ da $\mathbb{R}$ in $\mathbb{R}$ data da $\theta(x) = x^3$ e dimostriamo che θ è biunivoca. Basta mostrare che θ è crescente. Sia $x < y$. Vogliamo mostrare $x^3 < y^3$. Il caso difficile è quando x, y sono entrambi negativi. Ricordiamo che la moltiplicazione per un numero negativo rovescia le disuguaglianze. Da $x < y$ ottengo allora moltiplicando per x, $x^2 > xy$. Moltiplicando $x < y$ per y ottengo $xy > y^2$. Mettendo insieme le due disuguaglianze ottengo $x^2 > y^2$. Ora moltiplico questa per x e ottengo $x^3 < xy^2$. D'altra parte moltiplicando $x < y$ per il numero positivo y^2 ottengo $xy^2 < y^3$. Combinando le disuguaglianze ottenute ottengo $x^3 < y^3$.

5. Il grafico di una funzione

Siamo abituati a rappresentare una funzione $f : \mathbb{R} \to \mathbb{R}$ con un grafico sul piano cartesiano. In questo paragrafo discutiamo cosa è in generale il grafico di una funzione.

DEFINIZIONE 6.8. Consideriamo una funzione $f : X \to Y$. Il grafico di f è il sottoinsieme G_f di $X \times Y$ definito da

$$G_f = \{(x, y) \in X \times Y \mid y = f(x)\}$$

Equivalentemente possiamo dire che G_f è il sottoinsieme di $X \times Y$ definito da

$$G_f = \{(a, f(a)) \mid a \in X\}$$

Per esempio, consideriamo la funzione

$$f : \{1, 2, 3, 4\} \to \{1, 2, 3\}$$

definita da $f(1) = 3, f(2) = 2, f(3) = 3, f(4) = 3$. Il suo grafico è il sottoinsieme di $\{1, 2, 3, 4\} \times \{1, 2, 3\}$:

$$G_f = \{(1, 3), (2, 2), (3, 3), (4, 3)\}$$

che si può rappresentare con l' immagine di Figura 6 (dove abbiamo sistemato l'insieme $\{1, 2, 3, 4\}$ sulle "ascisse", l'insieme $\{1, 2, 3\}$ sulle "ordinate" e gli elementi del grafico sono quelli contrassegnati da una crocetta):

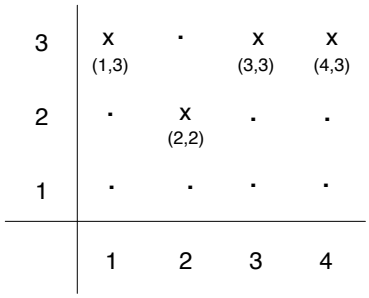

FIGURA 6. Il grafico di una funzione (la funzione descritta non è né iniettiva né surgettiva.)

Ci possiamo chiedere: dati due insiemi X e Y, quali sottoinsiemi del prodotto cartesiano $X \times Y$ possono essere interpretati come grafici di una qualche funzione che ha X come dominio e Y come codominio?

Ci rendiamo subito conto che non tutti i sottoinsiemi di $X \times Y$ hanno questa proprietà. Infatti, sia G_g il grafico di una funzione $g : X \to Y$; visto che la funzione associa ad ogni elemento di X uno ed un solo elemento di Y, G_g deve contenere, per ogni $a \in X$, uno ed un solo elemento (a, y), ossia con a come prima coordinata.

Detto "per immagini", se sistemiamo X sulle ascisse e Y sulle ordinate, l'intersezione della colonna relativa all'elemento a col nostro sottoinsieme G_g contiene esattamente un elemento.

Viceversa, se un sottoinsieme $\mathcal{L}$ di $X \times Y$ ha la caratteristica che, per ogni $x \in X$, esiste uno ed un solo elemento in $\mathcal{L}$ che ha x come prima coordinata, lo chiameremo "sottoinsieme di tipo grafico" e si vede subito che è possibile costruire una funzione $f : X \to Y$ che ha $\mathcal{L}$ come grafico.

Abbiamo dunque osservato che c'è una funzione bigettiva dall'insieme $F(X \to Y)$ di tutte le funzioni che hanno X come dominio e Y come codominio all'insieme di tutti i sottoinsiemi del cartesiano di tipo grafico.

Volendo esprimere questo fatto ancora con altre parole, possiamo dire che definire una funzione da X a Y equivale a descrivere un sottoinsieme di tipo grafico nel cartesiano $X \times Y$.

6. La composizione di funzioni

Dati tre insiemi X, Y e Z e due funzioni

$$f \,:\, X \to Y$$

$$g \,:\, Y \to Z$$

è possibile definire una nuova funzione che ha come dominio X e come codominio Z.

DEFINIZIONE 6.9. Dati X, Y, Z e f, g come sopra, la funzione g **composta con** f è la funzione

$$g \circ f \,:\, X \to Z$$

tale che, per ogni $x \in X$, $g \circ f(x) = g(f(x))$.

Osserviamo che, se $X = Y = Z$, le funzioni $f \circ g$ e $g \circ f$ hanno lo stesso dominio e lo stesso codominio (entrambi uguali a X, appunto). Possiamo chiederci: $f \circ g$ e $g \circ f$ sono la stessa funzione? In altri termini: questa operazione di composizione è *commutativa*? In generale, la risposta è no, come mostra il seguente esempio.

ESEMPIO 6.10. Siano

$$f \,:\, \mathbb{R} \to \mathbb{R} \qquad f(x) = x^3$$

$$g \,:\, \mathbb{R} \to \mathbb{R} \qquad f(x) = x + 2$$

Allora

$$f \circ g \,:\, \mathbb{R} \to \mathbb{R} \qquad f \circ g(x) = f(g(x)) = (x+2)^3$$

$$g \circ f \,:\, \mathbb{R} \to \mathbb{R} \qquad g \circ f(x) = g(f(x)) = x^3 + 2$$

e queste sono due funzioni sono diverse !

OSSERVAZIONE 6.11. Per x reale, $\sqrt{x^2} = |x|$.

7. Funzioni invertibili

Cominciamo ponendoci questa domanda. Se componendo due funzioni f e g ottengo la funzione identità, ossia la funzione che manda ogni elemento in sé stesso, cosa posso dire di f e di g?

PROPOSIZIONE 6.12. *Consideriamo due insiemi X, Y e due funzioni $f \,:\, X \to Y$, $g : Y \to X$. Se $g \circ f(u) = u$ per ogni elemento $u \in X$ allora g è surgettiva e f è iniettiva.*

DIMOSTRAZIONE. Se $f(u) = f(v)$ applicando g trovo $u = v$. Quindi f è iniettiva. Per risolvere $g(x) = b$, prendo $x = f(b)$. Quindi f è surgettiva. □

Siano $f(x) = x^2$ e $g(x) = \sqrt{x}$, prendendo come dominio e codominio di entrambe l'insieme $\mathbb{R}^{>0}$ dei reali positivi. Allora, per ogni $x \in \mathbb{R}^{>0}$, vale $f \circ g(x) = x$ e $g \circ f(x) = x$. Diciamo in questo caso che f, g sono l'una l'inversa dell'altra. Diamo la definizione in generale:

DEFINIZIONE 6.13. Sia $f \,:\, X \to Y$ una funzione dall'insieme X all'insieme Y. Si dice che f è invertibile se esiste una funzione $g \,:\, Y \to X$ che soddisfa le seguenti due condizioni:

(1) $g \circ f : X \to X$ è uguale alla funzione identità su X. In simboli:

$$g \circ f = Id_X : X \to X$$

(2) $f \circ g : Y \to Y$ è uguale alla funzione identità su Y. In simboli:

$$f \circ g = Id_Y : Y \to Y$$

TEOREMA 6.14. *Date due funzioni $f : X \to Y$, $g : Y \to X$, se f, g sono l'una l'inversa dell'altra, allora f, g sono bigettive. Inoltre, se $y \in Y$ risulta che $g(y)$ è la controimmagine di y tramite f (quindi l'inversa di una funzione biunivoca è unica).*

DIMOSTRAZIONE. Possiamo applicare la Proposizione 6.12 a $g \circ f$ e a $f \circ g$. La prima volta otteniamo che f è iniettiva e che g è surgettiva, la seconda volta che g è iniettiva e che f è surgettiva. Dunque f e g sono bigettive. Ora, preso $y \in Y$, sia $x \in X$ la sua controimmagine tramite f (cioè $f(x) = y$). Allora applicando g trovo $g(f(x)) = g(y)$ e dunque $g(y) = x$.

□

Abbiamo dunque osservato che una funzione invertibile è bigettiva. Vale anche il viceversa, come possiamo intuire facilmente. Riassumiamo queste osservazioni nel seguente teorema.

TEOREMA 6.15. *Sia $f : X \to Y$ una funzione dall'insieme X all'insieme Y. Allora f è invertibile se e solo se è bigettiva. Inoltre, se è invertibile, la sua inversa è unica.*

DIMOSTRAZIONE. Resta da dimostrare che se f è bigettiva allora è invertibile. Basta costruire l'inversa. Il Teorema 6.14 ci suggerisce come fare: definiamo una funzione $g : Y \to X$ ponendo, per ogni $y \in Y$, $g(y)$ uguale alla controimmagine di y tramite la f. Si verifica subito che una tale g soddisfa $g \circ f = Id_X$ e $f \circ g = Id_Y$.

□

8. Esercizi

ESERCIZIO 6.16. Sia $f\colon \mathbb{Q} \to \mathbb{Q}$ data da $g(x) = x^2$. Trovare le controimmagini di $0, 2, 4$.

ESERCIZIO 6.17. Sia $f\colon \mathbb{R} \to \mathbb{R}$ la funzione $f(x) = 3x - 2$. Determinare se f è iniettiva, surgettiva. Stessa domanda con $\mathbb{N}$ al posto di $\mathbb{R}$ come dominio e codominio.

ESERCIZIO 6.18. Sia $f\colon \mathbb{R} \to \mathbb{R}$ data da $f(x) = x^2$. Determinare se f è iniettiva, surgettiva. Siano $a < b$ in $\mathbb{R}$. Per quali valori di a, b la restrizione di f ad $[a, b]$ è iniettiva?

ESERCIZIO 6.19. Sia $f\colon \mathbb{R} \to \mathbb{R}$ data da $f(x) = (x - 3)^2 + 5$. Determinare se f è iniettiva, surgettiva. Per quali scelte di a e b, f ristretta ad $[a, b]$ è iniettiva?

ESERCIZIO 6.20. Sia $g\colon \mathbb{R} \to \mathbb{R}$ data da $g(x) = ax^2+bx+c$. Trovate le controimmagini di zero. Suggerimento: $4ag(x) = (2ax + b)^2 + (4ac - b^2)$. Determinare se g è surgettiva. Determinare per quali a, b la restrizione di g ad $[a, b]$ è iniettiva.

ESERCIZIO 6.21. Sia $f\colon \mathbb{R} \to \mathbb{R}$ data da $f(x) = x + 2^x$. Determinare se f è iniettiva.

ESERCIZIO 6.22. Sia $f\colon \mathbb{Z}^2 \to \mathbb{Z}$ data da $f(x, y) = x+y$. Determinare se f è iniettiva, surgettiva.

ESERCIZIO 6.23. Sia $f(x) = 3x + 5$ e $g(x) = 7x - 11$. Calcolare $f \circ g$ e $g \circ f$.

Esercizio 6.24. Consideriamo la funzione $g : \mathbb{R} \to \mathbb{R}$ data da

$$g(x) = 9x^2 - 6x + 2$$

Dire se è iniettiva, surgettiva o bigettiva. La stessa domanda per la funzione

$$g' : \mathbb{R}^{\geq 0} \to \{z \in \mathbb{R} \mid z \geq 1\}$$

data dalla stessa legge $g'(x) = 9x^2 - 6x + 2$.

Risoluzione. Studiamo innanzitutto la surgettività della g, ossia prendiamo un $y \in \text{Imm } g$ e studiamone le caratteristiche. Deve valere

$$y = 9x^2 - 6x + 2$$

per un qualche $x \in \mathbb{R}$. Si può anche riscrivere

$$y = (3x - 1)^2 + 1$$

da cui si nota subito che deve essere $y \geq 1$ (ossia $\text{Imm } g \subset \{z \in \mathbb{R} \mid z \geq 1\}$). Dunque la g non è surgettiva, perché ha sempre immagini di valore ≥ 1.

Studiamo la iniettività. Se $y \geq 1$, abbiamo

$$y - 1 = (3x - 1)^2$$

che ha senso perché $y - 1 \geq 0$ e possiamo ricavare

$$3x - 1 = \pm\sqrt{y - 1}$$

$$x = \frac{1 \pm \sqrt{y - 1}}{3}$$

Da questa espressione si ricava che se $y \geq 1$ allora $y \in \text{Imm } g$ (ossia $\text{Imm } g = \{z \in \mathbb{R} \mid z \geq 1\}$), perché abbiamo mostrato una formula per ricavare le sue controimmagini. In particolare si nota che $y = 1$ ha una sola controimmagine, ossia $\frac{1}{3}$. Se invece $y > 1$ allora ha due controimmagini distinte in $\mathbb{R}$. Dunque la g non è iniettiva.

Consideriamo adesso la g'. Sia y nel codominio di g', dunque $y \geq 1$. Vogliamo controllare se la g' è surgettiva, ossia se troviamo $x \in \mathbb{R}^{\geq 0}$ tale che

$$y = (3x - 1)^2 + 1$$

Provando a risolvere questa equazione si può scrivere, come abbiamo fatto prima,

$$x = \frac{1 \pm \sqrt{y - 1}}{3}$$

e, siccome fra le due soluzioni proposte ce ne è sempre una (la $x = \frac{1+\sqrt{y-1}}{3}$) che è ≥ 0 e dunque appartiene al dominio della g', si conclude che la g' è surgettiva.

Quanto alla iniettività, se dimostriamo che, per certi valori di $y > 1$, l'altra soluzione (la $x = \frac{1-\sqrt{y-1}}{3}$, che è distinta dalla prima per $y > 1$) è anch'essa nel dominio, avremo mostrato che la g' non è iniettiva.

Bisogna controllare quando

$$\frac{1 - \sqrt{y - 1}}{3} \geq 0$$

e troviamo che questa disuguaglianza è soddisfatta per $y \leq 2$. In conclusione, se scelgo un y tale che $1 < y \leq 2$, tale y ha due controimmagini secondo la g', che dunque non è iniettiva.

Osservazione. La funzione g ha il grafico dato da una parabola con punto di minimo per $x = \frac{1}{3}$ e valore minimo 1; il grafico permette di "leggere" bene i risultati provati qui sopra.

ESERCIZIO 6.25.

(i) La funzione
$$\begin{array}{rccc} f: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \mapsto & (2x+6y, x+3y) \end{array}$$
è iniettiva, surgettiva, bigettiva?

(ii) Al variare di $a, b \in \mathbb{R}$ la funzione
$$\begin{array}{rccc} f: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \mapsto & (2ax+6by, ax+3by) \end{array}$$
è iniettiva, surgettiva, bigettiva?

Risoluzione.

(i) La funzione non è iniettiva, infatti: $f(0,0) = 0$ e $f(3,-1) = (2\cdot 3 + 6\cdot(-1), 3 + 3\cdot(-1)) = (0,0)$. Proviamo ora che la funzione non è surgettiva. Osserviamo che abbiamo $f(x,y) = (2(x+3y), x+3y)$, cioè se un elemento $(u,v) \in \operatorname{Imm} f$ abbiamo $u = 2v$; in conclusione la funzione f non è surgettiva perchè ad esempio l'elemento $(1,0)$ non appartiene all'immagine di f. In particolare la funzione non è neanche bigettiva.

(ii) Vogliamo ora provare che per ogni $a, b \in \mathbb{R}$ la funzione f non è iniettiva e non è surgettiva. Infatti $f(3b,-a) = (2a\cdot 3b + 6b\cdot(-a), a\cdot 3b + 3b\cdot(-a)) = (0,0) = f(0,0)$, e quindi se la coppia $(a,b) \neq (0,0)$ allora la funzione f non è iniettiva visto che i due elementi distinti $(3b,-a)$ e $(0,0)$ hanno la stessa immagine. Se invece $a = b = 0$ allora abbiamo $f(x,y) = (0,0)$ per ogni $(x,y) \in \mathbb{R}^2$ e quindi f non è certamente iniettiva.

Proviamo ora che f non è surgettiva. Infatti per ogni $(x,y) \in \mathbb{R}^2$ abbiamo $f(x,y) = (2(ax+3by), ax+3by)$; allora per ogni elemento $(u,v) \in \operatorname{Imm} f$ abbiamo $u = 2v$. Quindi, ad esempio, l'elemento $(1,0)$ non è nell'immagine di f. In particolare la funzione f non è bigettiva.

ESERCIZIO 6.26. Dire, motivando la risposta, se la seguente è o no una definizione corretta di funzione:
$$g \,:\, \mathbb{Q} \to \mathbb{Z}\times\mathbb{Z}$$
tale che
$$\forall\, y \in \mathbb{Z} \qquad g(y) = (p,q) \text{ con } \; p \,\text{e}\, q \,\text{tali che } \frac{p}{q} = y$$

ESERCIZIO 6.27. Sia $f\colon \mathbb{R} \to \mathbb{R}$ la funzione definita da:
$$f(x) = \begin{cases} -2x & \text{se } |x| \leq 10, \\ x & \text{se } |x| > 10. \end{cases}$$
Determinare se f è iniettiva, surgettiva, bigettiva.

Esercizio 6.28. Definiamo $f\colon \mathbb{N} \to \mathbb{N}$ ponendo

$$f(x) = \begin{cases} 2\sqrt{x} & \text{se } x \text{ è un quadrato,} \\ 2x+1 & \text{se } x \text{ non è un quadrato} \end{cases}$$

Determinare se f è iniettiva, surgettiva, bigettiva.

Esercizio 6.29. (a) Sia $f : \mathbb{Q}\setminus\{0\} \to \mathbb{Q}$ la funzione definita da

$$f(x) = \frac{x-1}{x} \qquad \forall x \in \mathbb{Q}\setminus\{0\}.$$

La funzione f è iniettiva? La funzione f è surgettiva?

(b) Sia $g : \mathbb{Q}\setminus\{0,1\} \to \mathbb{Q}\setminus\{0,1\}$ la funzione definita da

$$g(t) = \frac{t-1}{t} \qquad \forall t \in \mathbb{Q}\setminus\{0,1\}.$$

Dimostrare che g è bigettiva e determinare le funzioni $g \circ g$, g^{-1}.

Esercizio 6.30. Sia $f\colon \mathbb{N}-\{0,1\} \to \mathbb{Z}$ la funzione definita nel seguente modo: se $n \in \mathbb{N}-\{0,1\}$ si decompone in fattori primi come $n = p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$ allora

$$f(n) = (-1)^{p_1}a_1p_1 + (-1)^{p_2}a_2p_2 + \cdots + (-1)^{p_n}a_np_n$$

Determinare se f è iniettiva, surgettiva, bigettiva.

Esercizio 6.31. Consideriamo la funzione $f : \mathbb{N} \to \mathbb{N}$ che è definita dalla seguente relazione: se $n \in \mathbb{N}$ ha la scrittura decimale

$$n = a_k a_{k-1} \cdots a_1 a_0$$

allora $f(n) = a_k 3^k + a_{k-1}3^{k-1} + \cdots + a_1 3 + a_0 3^0$. Dire se f è iniettiva, surgettiva, bigettiva.

Esercizio 6.32. Siano $f : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ e $g : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ le funzioni definite da

$$\begin{aligned} f(m,n) &= 2m + n^3 \qquad \forall (m,n) \in \mathbb{N}\times\mathbb{N}, \\ g(m,n) &= 3m + n^2 \qquad \forall (m,n) \in \mathbb{N}\times\mathbb{N}\ . \end{aligned}$$

Stabilire se f e g sono iniettive e/o surgettive.

Esercizio 6.33. Dati due insiemi X e Y e un sottoinsieme $A \subseteq X \times Y$ di tipo grafico, determinare (scrivendo le opportune proposizioni in linguaggio formale) quali caratteristiche deve avere A perché

- la funzione individuata da A sia iniettiva;
- la funzione individuata da A sia surgettiva;
- la funzione individuata da A sia bigettiva;
- la funzione individuata da A non sia né iniettiva né surgettiva;
- la funzione individuata da A non sia bigettiva.

Esercizio 6.34. Dati gli insiemi $X = \{1, 2, 3, 4, 5, 6, 7\}$ e $Y = \{1, 2, 3, 4, 5\}$, consideriamo il seguente sottoinsieme $B \subseteq X \times Y$:

$$B = \{(1, 4), (2, 2), (3, 5), (4, 1), (5, 5), (6, 2), (6, 3), (7, 5), (7, 6)\}$$

- B è di tipo grafico?
- Quante funzioni $f : X \to Y$ esistono tali che $G_f \subseteq B$?

Esercizio 6.35. Si considerino gli insiemi $A = \{1, 2, 3, 4, 5, 6\}$ e $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Quali dei seguenti sottoinsiemi di $A \times B$ possono essere ottenuti come grafici di una funzione da A a B?

$$C = \{(1, 2), (2, 3), (3, 4), (3, 5), (4, 6), (5, 7), (6, 8)\}$$

$$D = \{(1, 4), (2, 3), (3, 4), (4, 5), (5, 7)\}$$

$$E = \{(1, 9), (2, 8), (3, 7), (4, 6), (5, 6), (6, 6)\}$$

Data una funzione $f : A \to B$ e una funzione $g : B \to A$, è possibile che $g \circ f$ sia iniettiva? E che sia surgettiva? Stesse domande per la funzione $f \circ g$.

Esercizio 6.36. Siano dati due insiemi A e B e due funzioni

$$f : A \longrightarrow B \text{ e } g : B \longrightarrow A$$

Per ciascuna delle affermazioni seguenti, dimostrare che è vera o trovare un controesempio

(1) $f \circ g$ iniettiva implica f iniettiva.
(2) $f \circ g$ iniettiva implica g iniettiva.
(3) $f \circ g$ surgettiva implica f surgettiva.
(4) $f \circ g$ surgettiva implica g surgettiva.

Esercizio 6.37. Una funzione $f : \mathbb{R} \longrightarrow \mathbb{R}$ è pari se $\forall\ x \in A\ f(x) = f(-x)$. Una funzione $f : \mathbb{R} \longrightarrow \mathbb{R}$ è dispari se $\forall\ x \in A\ f(x) = -f(-x)$.

a) Dare un esempio di funzione pari e uno di funzione dispari.
b) Provare che la somma di funzioni pari è pari e che la somma di funzioni dispari è dispari.
c) Sia f pari e g dispari. Determinare la parità/disparità delle funzioni $f \circ g$, $g \circ f$.

Esercizio 6.38. Costruire una funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ che sia iniettiva e una $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ che sia surgettiva.

Esercizio 6.39. Si considerino i seguenti sottoinsiemi di $\mathbb{Z}$:

$$A = \{m \in \mathbb{Z} \mid m \text{ è un multiplo di } 3\}$$

$$B = \{n \in \mathbb{Z} \mid n^2 < 144\}$$

$$C = \{2z + 2 \mid z \in A\}$$

(1) Quanti elementi hanno gli insiemi $A \cap B$, $B \cap C$ e $A \cap B \cap C$?
(2) Si elenchino gli elementi dell'insieme

$$D = \{(x, y) \in (A \cap B) \times (B \cap C) \mid x \cdot y \leq 0\}$$

(3) Consideriamo la funzione $f : C \to A$ tale che $f(c) = c + 1$ per ogni $c \in C$. Dire se tale funzione è iniettiva, surgettiva, bigettiva.

Esercizio 6.40. Trovare, se esistono, le inverse delle funzioni $f : \mathbb{R} \to \mathbb{R}$ definita da $f(x) = 7x + 5$ e $g : \mathbb{R} \to \mathbb{R}$ definita da $g(x) = x^3 + 5$. Trovare inoltre una funzione $h : \mathbb{R} \to \mathbb{R}$ tale che $h \circ f : \mathbb{R} \to \mathbb{R}$ sia la funzione che manda ogni elemento $r \in \mathbb{R}$ nel suo quadrato.

Esercizio 6.41. Sia $f\colon \mathbb{N} \to \mathbb{N}$ definita da $f(x) = 2^x x$.

(1) Determinare se f è iniettiva, surgettiva, bigettiva.
(2) Calcolare la composizione $(f \circ f)(x)$.

Esercizio 6.42. Sia $f : \mathbb{R} \to \mathbb{R}$ la funzione data da

$$f(x) = x + \lfloor x \rfloor$$

dove $\lfloor x \rfloor$ è la parte intera (inferiore) di x, ossia il più grande numero intero $\leq x$.

a) Dire se f è iniettiva, surgettiva, bigettiva.

b) Trovare (se possibile!) una funzione $g : \mathbb{R} \to \mathbb{R}$ tale che, per ogni $x \in \mathbb{R}$, $g \circ f(x) = x$ e una funzione $h : \mathbb{R} \to \mathbb{R}$ tale che per ogni $x \in \mathbb{R}$, $f \circ h(x) = x$.

CAPITOLO 7

Calcolo combinatorio

1. La definizione di cardinalità e il lemma dei cassetti

Vogliamo discutere il concetto di cardinalità di un insieme (ossia la risposta alla domanda "quanti elementi ha ?"). In questo capitolo (e nel successivo) tratteremo il caso degli insiemi finiti.

Cominciamo col preparare una collezione di insiemi che avranno il ruolo di "insiemi campione"; per ogni $n \in \mathbb{N} - \{0\}$ poniamo:

$$\mathbb{N}_n = \{1, 2, 3, \ldots, n\}$$

A questo punto, lanciamo la:

DEFINIZIONE 7.1. Un insieme X è finito di cardinalità $n \in \mathbb{N} - \{0\}$ quando esiste una funzione bigettiva $g : X \to \mathbb{N}_n$. In tal caso si scrive che $|X| = n$. L'insieme vuoto è un insieme finito la cui cardinalità si pone uguale a 0; in simboli: $|\emptyset| = 0$.

DEFINIZIONE 7.2. Se un insieme non vuoto Y è tale che per nessun $n \in \mathbb{N} - \{0\}$ esiste una funzione bigettiva da Y a $\mathbb{N}_n$ allora si dice che Y è infinito.

Tutto a posto? In realtà non ancora: per essere sicuri che queste definizioni siano ben date, bisogna fare una verifica. Prendiamo infatti un insieme X che ammette una funzione bigettiva $f : X \to \mathbb{N}_n$. La definizione ci dice che allora X ha cardinalità n. Ma (domanda cattiva) siamo sicuri che non si possa trovare un'altra funzione bigettiva $g : X \to N_m$ con $m \neq n$? In tal caso avremmo un problema, il concetto di cardinalità non sarebbe definito univocamente.

L'intuizione ci rassicura: questo problema non accade. Formalmente quello che ci salva è il:

LEMMA 7.3 (Lemma dei cassetti, detto anche Lemma dei piccioni). *Supponiamo di avere una funzione $h : \mathbb{N}_n \to \mathbb{N}_m$ con $n > m$. Allora h non è iniettiva.*

Tale lemma si dimostra per induzione (per la dimostrazione, che non presentiamo qui, vedi per es. Eccles [**?**], capitolo 11).
Vediamo come mai il lemma "ci salva": supponiamo per assurdo di avere X, f, g come sopra; dato che $n \neq m$, possiamo pensare che $n > m$. Allora possiamo costruire la funzione

$$g \circ f^{-1} : \mathbb{N}_n \to \mathbb{N}_m$$

Tale funzione è invertibile, essendo composizione di due funzioni bigettive e dunque invertibili (la sua inversa è $f \circ g^{-1} : \mathbb{N}_m \to \mathbb{N}_n$). Dunque $g \circ f^{-1}$, essendo invertibile, è anche bigettiva; in particolare è iniettiva. Ma ciò è assurdo perché è in contraddizione col lemma dei cassetti.

Ora che abbiamo apprezzato l'importanza del lemma dei cassetti, rienunciamolo in un linguaggio più generale:

LEMMA 7.4 (Lemma dei cassetti - enunciato generale). *Supponiamo di avere una funzione $f : X \to Y$, dove X è un insieme di cardinalità n e Y è un insieme di cardinalità m, con $n > m$. Allora f non è iniettiva.*

Possiamo facilmente ricavare questo corollario (dimostrazione per esercizio !):

COROLLARIO 7.5. *Se N oggetti sono sistemati in K scatole, allora c'è (almeno) una scatola che contiene almeno $\lceil \frac{N}{K} \rceil$ oggetti (qui $\lceil \frac{N}{K} \rceil$ è la "parte intera superiore" di $\frac{N}{K}$, ossia il più piccolo numero intero $\geq \frac{N}{K}$).*

2. Prime applicazioni ed esempi

Ecco qualche altro enunciato che conferma fatti da noi facilmente intuibili. Le dimostrazioni formali sono lasciate come esercizio.

TEOREMA 7.6. *Supponiamo che X e Y siano insiemi tali che $X \subseteq Y$ e Y sia finito. Allora anche X è finito e $|X| \leq |Y|$.*

TEOREMA 7.7. *Supponiamo che $f : X \to Y$ sia una funzione fra insiemi finiti e non vuoti tali che $|X| < |Y|$. Allora f non è surgettiva.*

TEOREMA 7.8. *Supponiamo che X e Y siano insiemi finiti non vuoti della stessa cardinalità. Allora una funzione $f : X \to Y$ è iniettiva se e solo se è surgettiva.*

OSSERVAZIONE 7.9. Dunque, in questo caso dove $|X| = |Y|$, per provare che una certa funzione $g : X \to Y$ è bigettiva basta provare una sola fra queste due proprietà: g è iniettiva o g è surgettiva.

Concludiamo con due esempi di applicazioni "sofisticate" del lemma dei cassetti.

ESEMPIO 7.10. Dimostriamo che, dati $n+1$ numeri interi positivi distinti $a_1, a_2, \ldots, a_n, a_{n+1}$ minori o uguali a $2n$, fra questi numeri ce n' è uno che ne divide un altro.

Scriviamo ogni a_j come prodotto di una potenza di 2 per un numero dispari:

$$a_j = 2^{k_j} q_j$$

dove q_j è un numero positivo dispari e $k_j \in \mathbb{N}$. Allora i numeri $q_1, q_2, \ldots, q_n, q_{n+1}$ sono tutti dispari, positivi e minori di $2n$. Siccome ci sono solo n numeri dispari positivi minori di $2n$, per il lemma dei cassetti deve valere che due fra i numeri $q_1, q_2, \ldots, q_n, q_{n+1}$ sono uguali. Supponiamo per esempio che $q_1 = q_2$. Allora, ricordando che

$$a_1 = 2^{k_1} q_1 \qquad a_2 = 2^{k_2} q_2 = 2^{k_2} q_1$$

e che $k_1 \neq k_2$ (altrimenti a_1 e a_2 non sarebbero distinti) possiamo osservare che

- se $k_1 < k_2$ allora a_1 divide a_2,
- se $k_2 < k_1$ allora a_2 divide a_1.

ESEMPIO 7.11. Dimostrare che se mettiamo $n^2 + 1$ numeri reali distinti in una lista ordinata $(a_1, a_2, \ldots, a_{n^2+1})$, da tale lista possiamo estrarre una sottolista di $n+1$ numeri che risultano o strettamente crescenti o strettamente decrescenti[1].

[1]Per chiarire cosa intendiamo, consideriamo questo gioco: dopo aver scritto sulla lavagna una lista ordinata di n^2+1 numeri reali distinti, chiamo uno di voi e gli chiedo di fare un cerchietto intorno a $n+1$ di questi numeri. Dopo che ha fatto i cerchietti, cancello tutti gli altri numeri e lascio solo quelli cerchiati. Se questi numeri rimasti sono scritti in ordine strettamente decrescente o strettamente crescente, allora ho perso. L'enunciato dell'esercizio equivale a dire che questo è un bel gioco per voi, perché dice che, qualunque sia la lista che io ho scritto alla lavagna, c'è sempre un modo di farmi perdere.

Dimostriamolo per assurdo. Supponiamo che l'enunciato non sia vero. Allora, preso un qualunque numero x nella lista, consideriamo tutte le sottoliste crescenti che possiamo estrarre e che hanno x come primo elemento. Tali sottoliste devono essere composte da al massimo n elementi, altrimenti l'enunciato sarebbe vero. Prendiamo una di queste sottoliste che abbia lunghezza massima possibile e chiamiamo c_x la sua lunghezza, ossia il numero dei suoi elementi. Allo stesso modo, chiamiamo d_x la massima lunghezza di una sottolista strettamente decrescente con primo elemento x. Anche d_x deve essere $\leq n$. Possiamo dunque associare ad ogni elemento x della nostra lista un elemento di $\mathbb{N}_n \times \mathbb{N}_n$, esattamente la coppia (c_x, d_x). Per il lemma dei cassetti, visto che la lista contiene n^2+1 elementi e che la cardinalità di $\mathbb{N}_n \times \mathbb{N}_n$ è n^2, devono esistere due elementi distinti della lista, diciamo a_s e a_t, con $s < t$, a cui viene associata la stessa coppia, ossia tali che $(c_{a_s}, d_{a_s}) = (c_{a_t}, d_{a_t})$. Ora supponiamo che $a_s > a_t$. Allora, poiché a partire da a_t si può estrarre una sottolista di d_{a_t} numeri strettamente decrescenti, questo vuol dire che a partire da a_s si può estrarre una sottolista di almeno $d_{a_t}+1$ numeri strettamente decrescenti, semplicemente aggiungendo a_s alla sottolista che partiva da a_t. Dunque, per la definizione di d_{a_s}, deve essere $d_{a_s} \geq d_{a_t}+1$. Questo è ASSURDO visto che a_s e a_t erano tali che tali che $(c_{a_s}, d_{a_s}) = (c_{a_t}, d_{a_t})$, che in particolare implica $d_{a_s} = d_{a_t}$. In modo simile si trova un assurdo se $a_s < a_t$.

3. Insiemi di funzioni

Siano X e Y due insiemi. Chiamiamo $F(X \to Y)$ l'insieme di tutte le funzioni che hanno X come dominio e Y come codominio:

$$F(X \to Y) = \{f \mid f : X \to Y \quad \text{è una funzione}\}$$

Fedeli al tema di questo capitolo, ossia il "contare", ci chiediamo subito: quanti sono gli elementi di $F(X \to Y)$, ossia quante sono tutte le possibili funzioni che hanno X come dominio e Y come codominio?

TEOREMA 7.12. *Siano X e Y finiti non vuoti con $|X| = n$ e $|Y| = m$. Allora*

$$|F(X \to Y)| = m^n$$

DIMOSTRAZIONE. Sia $X = \{x_1, x_2, \dots x_n\}$ e $Y = \{y_1, y_2, \dots y_m\}$. Proviamo a costruire una funzione da X a Y.
Dove mandiamo x_1 ? Abbiamo m scelte: $y_1, y_2, \dots y_m$.
Dove mandiamo x_2 ? Abbiamo sempre m scelte: $y_1, y_2, \dots y_m$, perché non abbiamo fatto nessuna richiesta sulla funzione (tipo "che sia iniettiva" o "surgettiva" etc...).
In generale, dove mandiamo x_i con $i = 1, 2, \dots, n$? Abbiamo sempre m scelte.
Dunque alla fine possiamo costruire la nostra funzione in $\underbrace{m \cdot m \cdot m \cdots m}_{n \text{ volte}} = m^n$ modi diversi. □

Ripensiamo alla dimostrazione appena svolta: come mai se avevamo m scelte e poi ancora m scelte e poi ancora m scelte..... alla fine abbiamo moltiplicato $\underbrace{m \cdot m \cdot m \cdots m}_{n \text{ volte}}$?
Siccome ci capiterà di ripetere spesso ragionamenti simili a questo, vale la pena soffermarsi e riscrivere la dimostrazione da un altro punto di vista.

DIMOSTRAZIONE. In realtà individuare una funzione $f : X \to Y$ equivale ad individuare un elemento del prodotto cartesiano $\underbrace{Y \times Y \times \cdots \times Y}_{n \text{ volte}} = Y^n$. Infatti un elemento di Y^n è una lista $(a_1, a_2, \dots, a_n)$ di elementi di Y e per ogni tale lista noi possiamo porre

$f(x_1) = a_1, f(x_2) = a_2, \ldots, f(x_n) = a_n$. Viceversa, data una funzione $f : X \to Y$ possiamo costruire l'elemento $(f(x_1), f(x_2), \ldots, f(x_n)) \in Y^n$.

Dunque vale $|F(X \to Y)| = |Y^n|$ e noi abbiamo già osservato (vedi Paragrafo 3) del Capitolo 4) che $|Y^n| = m^n$ (in realtà in quel paragrafo abbiamo osservato che se A e B sono insiemi finiti allora $|A \times B| = |A| \cdot |B|$, da cui per induzione si ottiene subito la formula per la cardinalità del prodotto cartesiano di m insiemi). □

Chiamiamo ora $Inj\ (X \to Y)$ l'insieme di tutte le funzioni iniettive che hanno X come dominio e Y come codominio:

$$Inj\ (X \to Y) = \{f \mid f : X \to Y \quad \text{è una funzione iniettiva } \}$$

TEOREMA 7.13. *Siano X e Y finiti non vuoti con $|X| = n$ e $|Y| = m$. Allora*

$$|Inj\ (X \to Y)| = m(m-1)(m-2)\cdots(m-n+1)$$

DIMOSTRAZIONE. Sia $X = \{x_1, x_2, \ldots x_n\}$ e $Y = \{y_1, y_2, \ldots y_m\}$. Se $n > m$ il lemma dei Cassetti ci dice che $|Inj\ (X \to Y)| = 0$.
Supponiamo allora $n \leq m$ e proviamo a costruire una funzione iniettiva g da X a Y.
Dove mandiamo x_1 ? Abbiamo m scelte: $y_1, y_2, \ldots y_m$.
Dove mandiamo x_2 ? Abbiamo $m-1$ scelte, ossia gli elementi di $Y - \{g(x_1)\}$, visto che la funzione deve essere iniettiva.
In generale, dove mandiamo x_i con $i = 1, 2, \ldots, n$? Abbiamo $m - (i-1)$ scelte, cioè gli elementi di $Y - \{g(x_1), g(x_2), \ldots, g(x_{i-1})\}$. In particolare per l'ultimo elemento x_n avremo $m - (n-1)$ scelte.

Dunque alla fine possiamo costruire la nostra funzione in

$$m \cdot (m-1) \cdot (m-2) \cdots (m-n+1)$$

modi diversi.

Come ultima osservazione notiamo che la formula ottenuta vale per ogni m e ogni n interi positivi, ossia

$$|Inj\ (X \to Y)| = m(m-1)(m-2)\cdots(m-n+1)$$

si adatta bene anche al caso in cui $n > m$: in tal caso infatti la nostra formula è un prodotto di fattori fra i quali è presente anche $m - m$ e dunque ha come risultato 0 che, come abbiamo osservato all'inizio, è proprio il numero di funzioni iniettive da X a Y. □

Se $|X| = |Y|$ allora l'insieme delle funzioni bigettive che hanno X come dominio e Y come codominio è non vuoto. Chiamiamolo $Bij\ (X \to Y)$:

$$Bij\ (X \to Y) = \{f \mid f : X \to Y \quad \text{è una funzione bigettiva } \}$$

Come caso particolare del teorema appena dimostrato abbiamo:

TEOREMA 7.14. *Siano X e Y finiti non vuoti con $|X| = |Y| = n$. Allora*

$$|Bij\ (X \to Y)| = n!$$

DIMOSTRAZIONE. Visto che $|X| = |Y|$ allora $Bij\ (X \to Y) = Inj\ (X \to Y)$ e dunque si tratta solo di porre $n = m$ nell'enunciato del teorema precedente. □

4. La cardinalità dell'insieme delle parti di un insieme finito

Dato un insieme A, cominciamo col ricordare la definizione, data nel Paragrafo 6 del Capitolo 4, di "insieme delle parti di A". L'insieme $\mathcal{P}(A)$ delle parti di A è l'insieme i cui elementi sono tutti i sottoinsiemi di A:

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Osserviamo in particolare che $A \in \mathcal{P}(A)$ e $\emptyset \in \mathcal{P}(A)$. In questo paragrafo vogliamo contare quanti elementi ha $\mathcal{P}(A)$ nel caso in cui A sia un insieme finito.

TEOREMA 7.15. *Se* $|A| = n$ *allora* $|\mathcal{P}(A)| = 2^n$

DIMOSTRAZIONE. Se $A = \emptyset$ allora ho solo un sottoinsieme, e la formula torna. Se $|A| \geq 1$, per contare quanti sono i sottoinsiemi di A immaginiamo di doverne costruire uno. Osserviamo che per individuare un sottoinsieme basta sapere, per ognuno degli n elementi di A, se tale elemento appartiene o no al sottoinsieme. Possiamo dunque passare in rassegna gli elementi di A e per ognuno di loro abbiamo due scelte: SI (sta nel sottoinsieme) oppure NO. Dunque ci sono 2^n distinti sottoinsiemi di A. Osserviamo che l'insieme vuoto corrisponde al caso in cui abbiamo ricevuto sempre la risposta NO e l'insieme A al caso in cui abbiamo ricevuto sempre la risposta SI. □

OSSERVAZIONE 7.16. Possiamo riformulare la dimostrazione appena svolta dicendo che contare i sottoinsiemi di A equivale a contare le funzioni da A all'insieme di 2 elementi $\{SI, NO\}$. Per il Teorema 7.12 sappiamo che queste sono 2^n.

Proponiamo una seconda dimostrazione del Teorema; è una dimostrazione per induzione che riteniamo significativa.

DIMOSTRAZIONE. Applichiamo il principio di induzione per provare la proposizione T: "per ogni $n \in \mathbb{N}$, se un insieme A ha n elementi, l'insieme delle parti $\mathcal{P}(A)$ ne ha 2^n".

Il predicato $Q(n)$ in questo caso è: "se un insieme A ha n elementi, l'insieme delle parti $\mathcal{P}(A)$ ne ha 2^n".

PASSO BASE: si verifica che $Q(0)$ è vera. Infatti $Q(0)$ dice che l'insieme $\mathcal{P}(\emptyset)$ ha 2^0 elementi. Questo è vero perché $\mathcal{P}(\emptyset) = \{\emptyset\}$ e dunque possiede 1 elemento.

PASSO INDUTTIVO: sia $k \in \mathbb{N}$. Bisogna dimostrare che è vera l'implicazione

$$Q(k) \to Q(k+1)$$

Questo significa che prendiamo per vero che l'insieme delle parti di un insieme con k elementi ha 2^k elementi (è l'ipotesi induttiva) e dobbiamo dimostrare che, se prendiamo un insieme Y con $k+1$ elementi, allora l'insieme $\mathcal{P}(Y)$ ne ha 2^{k+1}.

Sia dunque

$$Y = \{y_1, y_2, \ldots, y_n, y_{n+1}\}$$

Scegliamo un elemento di Y, diciamo y_1. Osserviamo che i sottoinsiemi di Y sono di due tipi:

—tipo I: sottoinsiemi che contengono y_1.

—tipo II: sottoinsiemi che non contengono y_1.

I sottoinsiemi di tipo II, visto che non contengono y_1, coincidono con i sottoinsiemi di

$$\{y_2, \ldots, y_n, y_{n+1}\}$$

che è un insieme di n elementi. Per l'ipotesi induttiva sappiamo dunque che i sottoinsiemi di tipo II sono 2^n.

I sottoinsiemi di tipo I sono anch'essi 2^n. Infatti per costruirli tutti possiamo fare così: prendiamo un sottoinsieme $C \subseteq \{y_2, \ldots, y_n, y_{n+1}\}$ e gli aggiungiamo y_1:

$$C \cup \{y_1\}$$

Quindi abbiamo tanti insiemi di tipo I quanti sono i sottoinsiemi di $\{y_2, \ldots, y_n, y_{n+1}\}$ e, ancora per l'ipotesi induttiva, $|\mathcal{P}(\{y_2, \ldots, y_n, y_{n+1}\})| = 2^n$.

In conclusione, gli elementi di $\mathcal{P}(Y)$ sono $2^n + 2^n$ ossia 2^{n+1}, e questo termina la verifica del passo induttivo. □

5. I coefficienti binomiali

Dato un insieme X finito o infinito, costruiamo dei particolari sottoinsiemi del suo insieme delle parti $\mathcal{P}(X)$.

DEFINIZIONE 7.17. Dato $r \in \mathbb{N}$, chiamiamo $\mathcal{P}_r(X)$ l'insieme i cui elementi sono tutti i sottoinsiemi di X che hanno cardinalità r:

$$\mathcal{P}_r(X) = \{A \mid A \subseteq X \ \wedge \ |A| = r\}$$

Ora ci poniamo la domanda: se X è finito di cardinalità n, quanti elementi avrà $\mathcal{P}_r(X)$? Certamente $|\mathcal{P}_r(X)|$ sarà un numero naturale $\leq 2^n$, visto che se $r \leq n$ vale $\mathcal{P}_r(X) \subseteq \mathcal{P}(X)$ e se $r > n$ allora $\mathcal{P}_r(X)$ è vuoto .

Capire che numero è $|\mathcal{P}_r(X)|$ significa sapere quanti sono i possibili sottoinsiemi di r elementi di un insieme che ha n elementi. Questa informazione è cruciale nelle strategie che servono per "contare"; perciò $|\mathcal{P}_r(X)|$ merita un nome e un simbolo:

DEFINIZIONE 7.18. Indicheremo $|\mathcal{P}_r(X)|$ con il simbolo $\binom{n}{r}$ (si legge: "coefficiente binomiale n su r").

Quindi, per esempio, se abbiamo un mazzo di 40 carte, diremo che ad un giocatore possono capitare $\binom{40}{5}$ diverse "mani" di 5 carte. Tra poco sapremo anche calcolare questo numero.

Cominciamo comunque subito ad osservare alcune proprietà dei coefficienti binomiali:

- $\binom{n}{0} = 1$ per ogni $n \in \mathbb{N}$. Infatti dato un qualunque insieme finito X, questo ha un solo sottoinsieme con 0 elementi, ossia l'insieme vuoto. In particolare vale $\binom{0}{0} = 1$. Similmente si nota che $\binom{n}{n} = 1$ per ogni $n \in \mathbb{N}$.
- se $r > n$ allora $\binom{n}{r} = 0$. Infatti se X ha n elementi, non c'è nessun sottoinsieme di X con $r > n$ elementi.
- $\binom{n}{1} = n$ per ogni $n \in \mathbb{N}$. Infatti se $n = 0$ si ricade nel punto precedente, se invece $n \geq 1$ allora si osserva che, dato X con n elementi, i suoi sottoinsiemi di cardinalità 1 sono solo i "singoletti" del tipo $\{a\}$, al variare di $a \in X$.
- $\binom{n}{n-1} = n$ per ogni $n \in \mathbb{N}^+$. Infatti, per n positivo deve valere $\binom{n}{n-1} = \binom{n}{1}$: dato X con n elementi, i suoi sottoinsiemi di cardinalità 1 sono tanti quanti i sottoinsiemi di cardinalità $n-1$. La corrispondenza biunivoca è data dall'operazione di prendere il complementare.

- Più in generale, dato $0 \leq r \leq n$, vale che $\binom{n}{r} = \binom{n}{n-r}$. Anche questa volta l'operazione di prendere il complementare stabilisce una corrispondenza biunivoca fra i sottoinsiemi di X con r elementi e quelli con $n-r$ elementi.

Ecco finalmente una formula esplicita per $\binom{n}{r}$:

TEOREMA 7.19. *Dati $n, r \in \mathbb{N}$, con $0 \leq r \leq n$, vale che*

$$\binom{n}{r} = \frac{n\ (n-1)\ (n-2)\ \cdots (n-r+1)}{r!} = \frac{n!}{r!\ (n-r)!}$$

OSSERVAZIONE 7.20. Ricordiamo che qui, come in tutto il resto del corso, stiamo usando la convenzione per cui $0! = 1$. Dunque la formula conferma, come già sappiamo, che $\binom{n}{0} = \binom{n}{n} = \frac{n!}{0!\ n!} = 1$.

DIMOSTRAZIONE. Come prima, fissato un insieme X con n elementi, cerchiamo di contare la cardinalità di $\mathcal{P}_r(X)$. Consideriamo $\mathbb{N}_r = \{1, 2, 3, \ldots, r\}$ e una funzione iniettiva

$$f\ :\ \mathbb{N}_r \longrightarrow X$$

Chi è Imm f ? È un sottoinsieme di X di cardinalità r, dunque è un elemento di $\mathcal{P}_r(X)$, proprio uno di quelli che dobbiamo "contare".

Sarà vero che ogni elemento di $\mathcal{P}_r(X)$ lo posso esprimere come immagine di una funzione iniettiva da N_r a X ? Sì, preso infatti un elemento di $\mathcal{P}_r(X)$, cioè un sottoinsieme $\{a_1, a_2, \ldots, a_r\} \subseteq X$, posso facilmente indicare una funzione iniettiva da N_r a X la cui immagine sia proprio $\{a_1, a_2, \ldots, a_r\}$: per esempio posso prendere la $g\ :\ \mathbb{N}_r \longrightarrow X$ definita da $g(1) = a_1, g(2) = a_2, \ldots, g(r) = a_r$.

Insomma, con le funzioni iniettive da $\mathbb{N}_r$ a X "raggiungiamo" tutti gli elementi di $\mathcal{P}_r(X)$. Per trovare $|\mathcal{P}_r(X)|$ potremmo allora cominciare a contare $|Inj\ (\mathbb{N}_r \to X)|$, ossia quante sono le funzioni iniettive da $\mathbb{N}_r$ a X. Ma questo numero lo abbiamo già calcolato nel Teorema 7.13: è $n\ (n-1)\ (n-2)\ \cdots (n-r+1)$.

È vero allora che $|\mathcal{P}_r(X)| = n\ (n-1)\ (n-2)\ \cdots (n-r+1)$? NO, perché se scriviamo così commettiamo l'errore di contare ogni elemento di $\mathcal{P}_r(X)$ più volte. Precisamente, dato un sottoinsieme $\{a_1, a_2, \ldots, a_r\} \subseteq X$ lo stiamo contando $|Inj\ (\mathbb{N}_r \to \{a_1, a_2, \ldots, a_r\})|$ volte, cioè tante volte quante sono le diverse funzioni iniettive possibili da $\mathbb{N}_r$ a $\{a_1, a_2, \ldots, a_r\}$. Ma sappiamo quanto vale $|Inj\ (\mathbb{N}_r \to \{a_1, a_2, \ldots, a_r\})|$: applicando la formula per il conto delle funzioni iniettive a questo caso particolare in cui dominio e codominio hanno la stessa cardinalità r (dunque stiamo in realtà considerando le funzioni bigettive), troviamo che $|Inj\ (\mathbb{N}_r \to \{a_1, a_2, \ldots, a_r\})| = |Bij\ (\mathbb{N}_r \to \{a_1, a_2, \ldots, a_r\})| = r!$.

Allora, visto che col numero $n\ (n-1)\ (n-2)\ \cdots (n-r+1)$ abbiamo contato $r!$ volte ogni elemento di $\mathcal{P}_r(X)$, per avere $|\mathcal{P}_r(X)|$ basterà dividerlo per $r!$:

$$\binom{n}{r} = |\mathcal{P}_r(X)| = \frac{n\ (n-1)\ (n-2)\ \cdots (n-r+1)}{r!}$$

□

Possiamo ora tornare all'esempio delle carte da gioco, e concludere che, se abbiamo un mazzo di 40 carte, ad un giocatore possono capitare

$$\binom{40}{5} = \frac{40!}{5!\ 35!} = \frac{40 \cdot 39 \cdot 38 \cdot 37 \cdot 36}{5!} = 658008$$

diverse "mani" di 5 carte.

6. Contare con i binomiali: esempi

In questo paragrafo presentiamo alcuni esempi di problemi di calcolo combinatorio, in cui giocano un ruolo importante i coefficienti binomiali.

Le partizioni di un numero: un primo assaggio

Dato un intero n, quante sono le triple (x, y, z) di interi non negativi che verificano $x + y + z = n$?

SOLUZIONE: Cominciamo, a sorpresa, ponendoci un'altra domanda: se devo mettere in fila n palline bianche uguali fra loro e due nere (sempre uguali fra loro), in quanti modi posso farlo? La risposta è $\binom{n+2}{2}$ perché basta scegliere le due posizioni (fra le $n+2$ posizioni della fila) in cui mettere le due palline nere. Ora, le due domande che abbiamo considerato "contano" lo stesso numero, dunque anche la risposta al problema delle triple è $\binom{n+2}{2}$. Questo procedimento è tipico dei problemi del contare: per contare quanti elementi ha un insieme, se ne considera un altro che sappiamo avere la stessa cardinalità ma in cui sappiamo "contare" meglio. Nel caso in questione, ci resta da spiegare perché le due domande conducono alla stessa risposta. Una fila in cui compaiono n palline bianche e due palline nere individua una tripla nel seguente modo (vedi Figura 1): chiamo x il numero palline bianche che trovo prima di incontrare la prima pallina nera, y il numero di palline bianche comprese fra le due palline nere, e infine z il numero di palline bianche che incontro dopo l'ultima pallina nera. Viceversa, data una tripla (x, y, z) di interi non negativi che verificano $x + y + z = n$ possiamo costruire una fila di n palline bianche e due palline nere ponendo prima x palline bianche, poi una nera, poi y bianche, poi una nera, e infine le restanti z bianche.

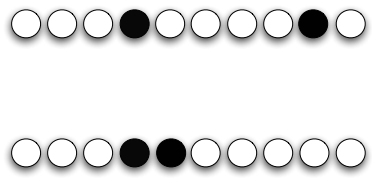

FIGURA 1. Due file di palline ("leggiamole" da sinistra a destra). Alla fila in alto associamo la tripla $(3, 4, 1)$ a quella in basso la tripla $(3, 0, 5)$.

□

Possiamo generalizzare subito questo risultato:

ESERCIZIO 7.21. Dato un numero naturale m e un numero intero positivo n, dimostrare che le n-uple $(x_1, x_2, \ldots, x_n)$ di numeri non negativi tali che $x_1 + x_2 + \cdots + x_n = m$ sono

$$\binom{m+n-1}{n-1}.$$

In altre parole, usando il linguaggio dei polinomi, questo è il numero dei possibili monomi di grado m nelle variabili $x_1, x_2, \ldots, x_n$.

Il poker

Supposto che le regole del poker a 52 carte (poker USA versione standard) siano note, determinare quante sono le mani che è possibile servire e che contengono:

(1) una qualunque configurazione (in sostanza qui si chiede quale è il numero delle mani distinte che è possibile servire).
(2) Scala reale massima.
(3) Scala reale.
(4) Colore.
(5) Scala.
(6) Nessun punto.
(7) Poker.
(8) Full.
(9) Tris.
(10) Doppia coppia.
(11) Una coppia.

SOLUZIONE: (1) Devo scegliere 5 carte su 52, senza ripetizioni, nessuna restrizione. Il numero che cerco è quindi il numero di sottoinsiemi di 5 elementi di un insieme di 52 elementi, quindi $\binom{52}{5}$.
(2) Per una scala reale massima le carte devono essere dello stesso seme, in scala e finire con un asso. Cè quindi una scala reale massima per ogni seme, quindi ce ne sono in totale 4.
(3) Per una scala reale, le carte devono essere tutte e 5 dello stesso seme, e la più grande può essere $5, 6, \ldots, A$, quindi ce ne sono 10 per seme. Per 4 semi, 40. Si ricorda che la scala reale minima ($A, 2, 3, 4, 5$ dello stesso seme) batte la massima.
(4) Per avere un colore, le 5 carte devono essere tutte dello stesso seme. Ne dobbiamo scegliere quindi 5 su 13, cioè $\binom{13}{5}$. Dato che ci sono 4 semi il numero di colori è $\binom{13}{5} \cdot 4$. Il numero dei colori che non sono una scala reale è $\binom{13}{5} \cdot 4 - 40$.
(5) Ci sono 10 sequenze di valori possibili per una scala. Dato che non abbiamo restrizioni sul seme da scegliere, il totale delle scale è $10 \cdot \binom{4}{1}^5$. Il numero delle scale non reali è $10 \cdot \binom{4}{1}^5 - 40$.
(6) Per non avere nessun punto, devo non avere nessun valore uguale e devo poi sottrarre al numero ottenuto il numero delle scale reali, delle scale e dei colori. Il numero di mani senza un valore ripetuto è $\binom{13}{5} \cdot \binom{4}{1}^5$. Infatti devo scegliere 5 valori su 13 e per ciascuno un seme su quattro.
(7) Poker: scelgo un valore su tredici $\binom{13}{1}$, quattro carte su quattro per quel valore $\binom{4}{4}$ e mi rimane una carta da scegliere su quarantotto $\binom{48}{1}$. Il numero totale è quindi $\binom{13}{1} \cdot \binom{4}{4} \cdot \binom{48}{1}$.
(8) Full: scelgo il primo valore, quello per il tris, in $\binom{13}{1}$ modi; posso scegliere le tre carte del tris in $\binom{4}{3}$ modi diversi. Scelgo il valore per la coppia, (uno sui dodici rimanenti) $\binom{12}{1}$. Posso scegliere le due carte della coppia in $\binom{4}{2}$ modi diversi. Il numero totale è quindi $\binom{13}{1} \cdot \binom{4}{3} \cdot \binom{12}{1} \cdot \binom{4}{2}$.
(9) Tris: scelgo un valore su tredici $\binom{13}{1}$; posso scegliere queste tre carte su quattro in $\binom{4}{3}$ modi diversi. Per le restanti due carte, devo avere: nessuna coppia, su le 48 carte rimanenti (48 e non 49 perchè voglio evitare di contare anche i poker

che potrebbero essere generati da un tris). Devo quindi scegliere due valori su dodici $\binom{12}{2}$ senza restrizioni sul seme $\binom{4}{1}^2$. Il totale è $\binom{13}{1} \cdot \binom{4}{3} \cdot \binom{12}{2} \cdot \binom{4}{1}^2$.

(10) Doppia coppia: scelgo il valore delle coppie $\binom{13}{2}$; posso scegliere le due carte in $\binom{4}{2}$ modi diversi per la prima coppia e similmente per la seconda. Scelgo il valore della carta rimanente $\binom{11}{1}$; posso scegliere questa carta in $\binom{4}{1}$ modi diversi. Il totale è quindi $\binom{13}{2} \cdot \binom{4}{2}^2 \cdot \binom{11}{1} \cdot \binom{4}{1}$.

(11) Coppia: Scelgo il valore della coppia $\binom{13}{1}$; posso scegliere le due carte in $\binom{4}{2}$ modi diversi. Per le restanti tre carte, scelgo tre valori distinti $\binom{12}{3}$. Non ho restrizioni sul seme di queste tre carte, quindi il fattore è $\binom{4}{1}^3$. Il totale è quindi $\binom{13}{1} \cdot \binom{4}{2} \cdot \binom{12}{3} \cdot \binom{4}{1}^3$.

□

Osservazione 7.22. Un altro modo di calcolare il numero di mani che mi dà un tris è: in un tris ci devono essere tre valori distinti, che posso quindi scegliere in $\binom{13}{3}$ modi diversi. Posso scegliere le carte del tris in $\binom{4}{3}$ modi diversi, e le due carte rimanenti in $\binom{4}{1}$ modi ciascuna. Devo ancora considerare che devo scegliere quale dei tre valori scelti sia quello del tris, e questo posso farlo in 3 modi diversi. Il numero totale è quindi

$$\binom{13}{3} \cdot \binom{4}{3} \cdot \binom{4}{1}^2 \cdot 3$$

Osservazione 7.23. Notiamo che le mani con un full sono 3744 mentre quelle con un colore sono 5108, in concordanza col fatto che nel poker americano il full batte il colore. Cosa accade nel poker "italiano", per esempio se le carte a disposizione sono solo 7,8,9,10, jack, donna, re e asso ?

Un cono dal gelataio.

Un gelataio ha 20 gusti di gelato, 12 alla frutta e 8 non di frutta.
a) In quanti modi si può fare un cono con 4 gusti ?
b) In quanti modi si può fare un cono con 4 gusti, di cui almeno due di frutta ?
c) In quanti modi si può fare un cono con 4 gusti, di cui almeno due di frutta, ma in cui non si trovano insieme il limone e il fiordilatte ?

Soluzione: a) In $\binom{20}{4}$ modi, si tratta infatti di scegliere 4 elementi in un insieme di 20.

b) Qui bisogna stare attenti, conviene contare il complementare: infatti se dai $\binom{20}{4}$ coni possibili togliamo gli $\binom{8}{4}$ coni senza frutta e i $12\binom{8}{3}$ coni in cui c'è esattamente un solo gusto di frutta, quelli che restano sono i coni con almeno due gusti di frutta, ossia proprio quelli che ci interessano. Dunque la risposta è $\binom{20}{4} - \binom{8}{4} - 12\binom{8}{3}$.

c) Anche qui conviene contare il complementare: se dai $\binom{20}{4} - \binom{8}{4} - 12\binom{8}{3}$ coni con almeno due gusti di frutta si levano quelli che hanno fiordilatte e limone insieme, i coni che restano sono proprio quelli che ci interessano. Quanti sono i coni con almeno due gusti di frutta che hanno fiordilatte e limone insieme? Visto che fiordilatte e limone ci sono, restano da decidere due palline. Se sono entrambe di frutta, si possono scegliere in $\binom{11}{2}$ modi. Se sono una di frutta (11 possibilità) e una non di frutta (7 possibilità), si possono scegliere in $11 \cdot 7$ modi. Ricordiamo che non contempliamo il caso in cui sono

entrambe non di frutta perché vogliamo che nel nostro cono ci siano almeno due gusti di frutta. Dunque la risposta è $\binom{20}{4} - \binom{8}{4} - 12\binom{8}{3} - \binom{11}{2} - 11 \cdot 7$. □

Estrazioni.

In una scatola vi sono 30 palline numerate da 1 a 30. Le palline da 1 a 10 sono colorate di rosso, le palline da 11 a 20 sono colorate di verde e le palline da 21 a 30 sono colorate di giallo. In quanti modi diversi si possono estrarre:

(i) 3 palline di diverso colore,
(ii) 3 palline dello stesso colore,
(iii) 3 palline di al più 2 colori.

N.B.: consideriamo come diversi due gruppi di palline con stessi colori ma diversi numeri.

SOLUZIONE: (i) Estrarre 3 palline di diverso colore significa estrarre una pallina rossa, una pallina verde ed una pallina gialla. Visto che le scelte sono indipendenti e che vi sono 10 palline per ogni colore, abbiamo 10^3 scelte possibili.

(ii) Abbiamo 3 modi di scegliere il colore e, una volta fissato il colore, basta estrarre 3 palline da un gruppo di 10 palline del colore fissato. Quindi il numero totale di scelte totale possibili è $3 \begin{pmatrix} 10 \\ 3 \end{pmatrix}$

(iii) Scegliere 3 palline di al più 2 colori è equivalente ad escludere le scelte con 3 palline di colore diverso. Allora visto che tutte le possibili estrazioni sono $\begin{pmatrix} 30 \\ 3 \end{pmatrix}$ abbiamo che le scelte cercate sono $\binom{30}{3} - 10^3$ per quanto visto sopra.

□

7. Il triangolo di Pascal-Tartaglia

Cominciamo questo paragrafo individuando una regola fondamentale che permette di costruire ricorsivamente i coefficienti binomiali.

TEOREMA 7.24. *Dati $r, n \in \mathbb{N}^+$ con $1 \leq r < n$, vale*

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

DIMOSTRAZIONE. Sia X un insieme con n elementi. Visto che $n \geq 1$, possiamo scegliere un elemento $a \in X$. Per calcolare $\binom{n}{r}$ dobbiamo calcolare la cardinalità di $\mathcal{P}_r(X)$. Possiamo adesso dividere $\mathcal{P}_r(X)$ in due parti[2], raggruppando in un sottoinsieme (che chiameremo L_1) tutti i sottoinsiemi di X di cardinalità r che contengono a, e in un altro (che chiameremo L_2) tutti i sottoinsiemi di X di cardinalità r che NON contengono a:

$$\mathcal{P}_r(X) = L_1 \cup L_2$$

Trattandosi di una unione di due insiemi disgiunti, vale che

$$\binom{n}{r} = |\mathcal{P}_r(X)| = |L_1| + |L_2|$$

[2]Al lettore non sfuggirà la somiglianza di questo argomento con quello usato nella seconda dimostrazione del Teorema 7.15..si tratta di una tecnica molto utile nei problemi enumerativi.

Ora, un sottoinsieme di cardinalità r che contiene a è univocamente determinato se si dice quali sono gli altri elementi (quelli diversi da a) che contiene; tali elementi costituiscono un sottoinsieme di cardinalità $r-1$ di $X-\{a\}$. Dunque

$$|L_1| = |\mathcal{P}_{r-1}(X-\{a\})| = \binom{n-1}{r-1}$$

Analogamente si osserva che scegliere un sottoinsieme di X di cardinalità r che non contiene a equivale a scegliere un sottoinsieme di $X-\{a\}$ di cardinalità r, dunque

$$|L_2| = |\mathcal{P}_r(X-\{a\})| = \binom{n-1}{r}$$

Allora possiamo concludere che

$$\binom{n}{r} = |\mathcal{P}_r(X)| = |L_1| + |L_2| = \binom{n-1}{r-1} + \binom{n-1}{r}$$

□

Il teorema che abbiamo appena dimostrato è il motivo per cui possiamo disporre i coefficienti binomiali in modo da formare il cosiddetto "Triangolo di Pascal-Tartaglia":

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
\ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots
\end{array}$$

Nella riga n-esima abbiamo collocato i coefficienti binomiali $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}$ (il vertice del triangolo lo consideriamo come la "riga 0-esima"). Dalla terza riga in poi, ogni numero interno al triangolo coincide appunto, come ci garantisce il teorema appena dimostrato, con la somma dei due numeri che si trovano sopra di lui.

8. Il teorema del binomio di Newton

Vediamo adesso perché i numeri $\binom{n}{r}$ si chiamano "coefficienti binomiali". Date due variabili a e b, consideriamo il binomio $(a+b)$ e le sue prime potenze:

$$(a+b)^0 = 1$$

$$(a+b)^1 = a+b$$

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

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

Come possiamo notare, i coefficienti che compaiono in questi sviluppi sono, riga per riga, gli elementi delle prime righe del Triangolo di Pascal -Tartaglia: 1, 1-1, 1-2-1, 1-3-3-1.

Questa osservazione vale in generale: i coefficienti dello sviluppo del binomio $(a+b)^n$ sono proprio i "coefficienti binomiali" $\binom{n}{r}$.

TEOREMA 7.25 (Teorema del binomio di Newton). *Date due variabili a e b, per ogni $n \in \mathbb{N}$ vale:*

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

cioè

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

DIMOSTRAZIONE. Cominciamo da un esempio, per avere un'idea di cosa succede. Calcoliamo lo sviluppo di $(a+b)^3$. Se non raggruppiamo i termini troviamo:

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

$$= aa(a+b) + ab(a+b) + ba(a+b) + bb(a+b) = aaa + aab + aba + abb + baa + bab + bba + bbb$$

Abbiamo espresso $(a+b)^3$ come somma di 8 monomi, ognuno dei quali è stato ottenuto, tramite le proprietà distributiva e associativa, scegliendo o a o b da ogni parentesi che compare in $(a+b)(a+b)(a+b)$.

Quindi, raggruppando adesso i termini tramite la proprietà commutativa, quale sarà il coefficiente di a^2b? Sarà uguale al numero dei monomi in cui troviamo due a e una b. E questi quanti sono ? Sono $3 = \binom{3}{2}$, ossia sono tanti quanti sono i modi di scegliere due parentesi fra le tre del prodotto $(a+b)(a+b)(a+b)$ (queste saranno le parentesi da cui prendo la a): la prima e la seconda, la prima e la terza, la seconda e la terza. Dunque nello sviluppo avremo $3a^2b$. Ovviamente, saremmo arrivati allo stesso risultato contando i modi di scegliere una parentesi fra le tre del prodotto $(a+b)(a+b)(a+b)$ (quella da cui prendo la b), perché $\binom{3}{1} = \binom{3}{2} = 3$.

Passiamo al caso generale. Nello sviluppo di $(a+b)^n$ troveremo 2^n monomi, ciascuno ottenuto scegliendo o a o b da ognuna delle n parentesi del prodotto

$$(a+b)^n = (a+b)(a+b)(a+b)\cdots(a+b)(a+b)$$

Raggruppando i termini, preso un indice i con $0 \leq i \leq n$, quale sarà allora il coefficiente di $a^{n-i}b^i$? Sarà uguale al numero di modi con cui si possono scegliere i parentesi fra le n del prodotto $(a+b)(a+b)(a+b)\cdots(a+b)(a+b)$ (quelle da cui prendiamo la b); dunque sarà uguale a $\binom{n}{i}$. Oppure sarà uguale al numero di modi con cui si possono scegliere $n-i$ parentesi fra le n del prodotto $(a+b)(a+b)(a+b)\cdots(a+b)(a+b)$ (quelle da cui prendiamo la a): infatti come sappiamo $\binom{n}{i} = \binom{n}{n-i}$. In conclusione, nello sviluppo di $(a+b)^n$ troveremo il termine $\binom{n}{i}a^{n-i}b^i$. Siccome questo è vero per ogni i, con $0 \leq i \leq n$, abbiamo dimostrato il teorema. □

9. Esercizi

ESERCIZIO 7.26. Dato un insieme X di cardinalità n, quante sono le coppie $(a,b) \in X \times X$ tali che $a \neq b$?
Quante sono le n-uple $(a_1, a_2, \ldots, a_n) \in X^n$ tali che $a_i \neq a_j$ per ogni $i \neq j$?
Qual è la cardinalità di $Inj\ (\mathbb{N}_2 \to X)$?
Qual è la cardinalità di $Inj\ (\mathbb{N}_n \to X)$?
Rispondere a queste quattro domande ed evidenziare i collegamenti fra di loro.

ESERCIZIO 7.27. Contare quante sono le funzioni surgettive da $\mathbb{N}_5$ a $\mathbb{N}_3$.

Esercizio 7.28. Descrivere una funzione da N_{15} a $\mathbb{N}_{15}$ che non sia bigettiva. Quante sono tali funzioni?

Esercizio 7.29. Sia $f\colon A \to B$ con A, B insiemi finiti, e supponiamo che ogni $b \in B$ abbia n controimmagini in A. Quale è il rapporto tra $|A|$ e $|B|$?

Esercizio 7.30. Quante sono le funzioni $f\colon \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ tali che per ogni x nel dominio di f si ha $f(x) \geq x$? Dimostrare per induzione un risultato generale.

Esercizio 7.31. Dimostrare che per ogni $n \in \mathbb{N}$ vale $\sum_{i=0}^{n} \binom{n}{i} = 2^n$ (in base a quanto abbiamo visto nel corso, ci sono varie dimostrazioni possibili..).

Esercizio 7.32. Dimostrare che per ogni $n \in \mathbb{N}$ vale $\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$.

Esercizio 7.33. Trovare il più piccolo intero positivo n_0 tale che la disuguaglianza

$$\sum_{i=1}^{n} \binom{n}{i} \geq n^2 + 3n$$

sia valida per tutti gli interi $n \geq n_0$ e dimostrare questo fatto per induzione.

Esercizio 7.34. Dimostrare che, per ogni intero positivo n vale

$$\sum_{i=0}^{n} i\binom{n}{i} = n2^{n-1}$$

Esercizio 7.35. Si consideri il numero

$$2^3 3^4 57^2 11^6 = 281253024360$$

- Quanti sono i suoi divisori in $\mathbb{Z}$?
- Quanti sono i suoi divisori che sono divisibili per 2 o per 3 ?

Esercizio 7.36. Si consideri l'insieme dei primi venti numeri interi positivi $A = \{1, 2, \ldots, 19, 20\}$. Diciamo che un sottoinsieme di A è misto se fra i suoi elementi ci sono almeno un numero pari e almeno un numero dispari.

- Quanti sono i sottoinsiemi di A che NON sono misti ?
- Quanti sono i sottoinsiemi misti che contengono esattamente 2 numeri pari ?
- Quanti sono i sottoinsiemi misti di cardinalità 7 ?

Esercizio 7.37. In uno stato le targhe delle macchine sono composte da 13 caratteri. Un carattere può essere una cifra (ossia 0,1,2,3,4,5,6,7,8,9) o la lettera A.
a) Quante sono le macchine che possono essere immatricolate ?
b) Quante sono le targhe che contengono esattamente tre A ?
c) Quante sono le targhe che contengono esattamente tre A consecutive ?
d) Quante sono le targhe che contengono esattamente tre A e che sono palindrome, ossia sono uguali se lette da sinistra a destra o da destra a sinistra ?

Esercizio 7.38. In una targa automobilistica compaiono due lettere, poi tre cifre e poi di nuovo due lettere, tipo: AX 456 TK. Sono ammesse le ripetizioni, le lettere sono scelte da un alfabeto di 26 lettere, le cifre possibili sono 0,1,2,3,4,5,6,7,8,9.
a) Quante sono tutte le possibili targhe?
b) Quante sono le targhe in cui c'è una lettera che compare esattamente tre volte?
c) Quante sono le targhe in cui c'è almeno una lettera che compare almeno due volte?
d) Quante sono le targhe in cui le cifre pari che compaiono sono di più delle cifre dispari?

Esercizio 7.39. Trenta studenti devono essere distribuiti in 3 classi: classe A, classe B e classe C. Quanti sono in modi di distribuire gli studenti nelle classi supponendo:

- che ogni classe deve contenere 10 studenti?
- che ogni classe può contenere un numero qualsiasi di studenti?
- che ogni classe può contenere un numero qualsiasi di studenti purché diverso da zero?

Esercizio 7.40. L'alfabeto italiano consiste di 21 lettere di cui 5 vocali e 16 consonanti. Quante parole di 7 lettere si possono formare:

- Supponendo di non poter usare due volte la stessa lettera?
- Supponendo di non poter utilizzare due volte la stessa vocale?
- Supponendo di non poter affiancare due lettere uguali?

Esercizio 7.41. Una gelateria ha 30 gusti di gelato, di cui 10 alla frutta.

- Quanti modi ci sono di scegliere un gelato di 3 gusti, di cui 2 alla frutta?
- Quanti modi ci sono di scegliere un gelato di 4 gusti, di cui almeno tre alla frutta?
- Quanti modi ci sono di scegliere un gelato di 3 gusti, di cui almeno due alla frutta, supponendo che limone e fiordilatte non possano andare insieme?

Esercizio 7.42. In una gelateria ci sono 10 gusti di gelato con cioccolato, 10 gusti di gelato alla crema e 10 gusti di gelato alla frutta.

- Quanti diversi coni con quattro gusti si possono preparare ?
- Quanti diversi coni con quattro gusti di cui almeno uno di crema, almeno uno di cioccolato e almeno uno di frutta si possono preparare ?
- Quanti coni con quattro gusti non tutti dello stesso tipo si possono preparare ?

Esercizio 7.43. Ad un compito, 300 studenti (150 maschi e 150 femmine), devono distribuirsi a gruppi di 100 in tre aule (A,B,C). N.B. Si considerano diverse due distribuzioni se i gruppi di studenti sono uguali ma le aule in cui sono distribuiti sono diverse.

- In quanti modi diversi si possono distribuire gli studenti ?
- In quanti modi diversi si possono distribuire gli studenti in modo che ci sia un'aula tutta di maschi ?
- In quanti modi diversi si possono distribuire gli studenti in modo che ci sia un'aula tutta di maschi e una tutta di femmine ?

Esercizio 7.44. Consideriamo il triangolo di Tartaglia scritto nel seguente modo:

$$\begin{array}{cccccccc}
1 & & & & & & & \\
1 & 1 & & & & & & \\
1 & 2 & 1 & & & & & \\
1 & 3 & 3 & 1 & & & & \\
1 & 4 & 6 & 4 & 1 & & & \\
1 & 5 & 10 & 10 & 5 & 1 & & \\
1 & 6 & 15 & 20 & 15 & 6 & 1 & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\
\binom{n}{0} & \binom{n}{1} & \binom{n}{2} & \dots & \dots & \dots & \dots & \binom{n}{n} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}$$

Dimostrare che, se si sommano i numeri sulle diagonali che da un 1 nella colonna di sinistra salgono verso destra, si ottengono i numeri della successione di Fibonacci.

Esercizio 7.45. Dobbiamo distribuire i numeri naturali che appartengono a $\mathbb{N}_{64} = \{1, 2, 3, \dots, 64\}$ su una scacchiera 8×8.

- In quanti modi diversi possiamo farlo ?
- In quanti modi diversi possiamo farlo se vogliamo che i numeri dispari stiano tutti su caselle dello stesso colore ?
- In quanti modi diversi possiamo farlo se vogliamo che tutti i multipli di 4 stiano su caselle nere ?
- In quanti modi diversi possiamo farlo se vogliamo che ogni colonna contenga esattamente 4 dispari ?

Esercizio 7.46. Ad una gara di ciclismo sono presenti 20 squadre di 9 corridori ciascuna. Si vogliono scegliere 22 corridori per un controllo antidoping preventivo:

- In quanti diversi modi si può scegliere il gruppo di corridori da controllare ?
- In quanti diversi modi si può scegliere il gruppo di corridori da controllare se si vuole controllare almeno un corridore per squadra ?
- In quanti diversi modi si può scegliere il gruppo di corridori da controllare se si vuole che ci sia una e una sola squadra della quale sono chiamati al controllo tutti i corridori ?

Esercizio 7.47. Sia $\mathbb{N}_{30} = \{1, 2, 3, 4, \dots, 28, 29, 30\}$.

- Quanti sono i sottoinsiemi di $\mathbb{N}_{30}$ che contengono esattamente tre numeri pari e quattro numeri dispari ?

- Quanti sono i sottoinsiemi di $\mathbb{N}_{30}$ che contengono un numero pari (positivo, non zero) di numeri pari ?

- Quanti sono i sottoinsiemi di $\mathbb{N}_{30}$ che contengono almeno tre numeri pari e due numeri dispari ?

ESERCIZIO 7.48. Consideriamo i numeri interi x tali che $10000000 \leq x < 20000000$.

a) In quanti di questi numeri, scritti in notazione decimale, la cifra 3 compare esattamente due volte?
b) In quanti di questi numeri, scritti in notazione decimale, le cifre che compaiono sono tutte diverse fra loro?
c) Quanti di questi numeri si scrivono (in notazione decimale) usando al più due cifre?

ESERCIZIO 7.49. Sia $A = \{1, 2, 3, 4, \ldots, 20\}$ e $B = \{1, 2, 3, 4, \ldots, 15\}$.
a) Quante sono le funzioni f da A in B tali che $f(x) \neq x$ per ogni $x \in A$?
b) Quante sono le funzioni da A in B che mandano numeri pari in numeri pari ?
c) Quante sono le funzioni da A in B tali che, per ogni $b \in B$, la controimmagine di b ha 0 oppure 2 elementi ?
d) Possono esistere delle funzioni da A in B tali che, per ogni $b \in B$, la controimmagine di b ha 0 oppure 3 elementi ?

ESERCIZIO 7.50. Vogliamo costruire un numero di 13 cifre, usando solo le cifre 1,2,3,4,5,6.

a) Quanti numeri possiamo costruire?
b) Quanti numeri possiamo costruire in cui compaiono almeno due cifre distinte?
c) Quanti numeri possiamo costruire in cui la cifra 1 compare esattamente quattro volte?
d) Quanti numeri possiamo costruire in cui compaiono più cifre pari che cifre dispari?

[Per evitare ambiguità in questa ultima domanda chiariamo per esempio che il numero 1111111111121 va considerato con 12 cifre dispari (anche se la cifra usata è sempre l'1) e una pari . Similmente, il numero 1112223334445 va considerato con sette cifre dispari e sei pari]

SOLUZIONE: a) Per ognuna delle tredici posizioni da occupare con una cifra abbiamo 6 scelte. Dunque possiamo costruire 6^{13} numeri distinti.

b) Conviene contare per complementare. I numeri in cui compaiono almeno due cifre sono tutti i numeri costruibili (che sono 6^{13}) eccetto i 6 numeri in cui si usa una sola delle cifre che abbiamo a disposizione. Dunque la risposta è $6^{13} - 6$.

c) Bisogna scegliere le 4 posizioni dove comparirà la cifra 1. Questo si può fare in $\binom{13}{4}$ modi. Nelle nove caselle rimanenti possiamo mettere una delle cifre

2,3,4,5,6. Abbiamo dunque 5^9 modi di completare la costruzione del numero. In conclusione la risposta è $\binom{13}{4}5^9$.

d) Qui conviene pensare alla simmetria generale del problema. Possiamo usare tre cifre pari (2,4,6) e tre cifre dispari (1,3,5) per costruire il nostro numero. Ogni numero che costruiamo avrà più cifre pari che cifre dispari o viceversa (non potrà capitare che abbia tante cifre pari quante dispari perché il numero ha tredici cifre). Questo ci permette di intuire che la risposta sarà

$$\frac{6^{13}}{2}$$

ossia i numeri con più cifre pari saranno la metà del totale.

Formalizziamo meglio questa intuizione, mostrando una funzione bigettiva fra l'insieme dei numeri da noi costruibili con più cifre pari e l'insieme di quelli con più cifre dispari. Sia $f : \{1,2,3,4,5,6\} \to \{1,2,3,4,5,6\}$ la funzione definita da $f(1) = 2, f(2) = 1, f(3) = 4, f(4) = 3, f(5) = 6, f(6) = 5$[3]. A questo punto, se

$$a_{12}a_{11}a_{10}a_9 \dots a_3a_2a_1a_0$$

è uno dei 6^{13} numeri che possiamo ottenere, lo mettiamo in corrispondenza col numero

$$f(a_{12})f(a_{11})f(a_{10})f(a_9) \dots f(a_3)f(a_2)f(a_1)f(a_0)$$

Potete facilmente verificare che questa corrispondenza descrive una funzione bigettiva fra l'insieme dei numeri da noi costruibili con più cifre pari e l'insieme di quelli con più cifre dispari. Notate che al posto della f avremmo potuto scegliere un'altra permutazione dei numeri 1,2,3,4,5,6 che manda pari in dispari e dispari in pari.

□

[3]Usando il linguaggio che introdurremo nel Paragrafo 3 sul gruppo simmetrico possiamo dire che f è la permutazione $(1,2)(3,4)(5,6)$.

CAPITOLO 8

Contare.... l'infinito

1. Prime osservazioni

Nel Capitolo 7 abbiamo dato la definizione di insieme infinito "per esclusione" (un insieme X è infinito quando non è finito..).

Quando consideriamo gli insiemi infiniti, una prima domanda naturale da porsi è se due insiemi infiniti si possono confrontare fra di loro, o, in altri termini, se si può stabilire se uno dei due è "più grande" dell'altro. Facciamo subito un esempio che ci fa capire come il concetto di "più grande" vada precisato.

PROPOSIZIONE 8.1. *Gli insiemi* $\mathbb{N}$ *e* $\mathbb{Z}$ *sono in corrispondenza biunivoca. Gli insiemi* $\mathbb{N}$ *e* $\mathbb{N}^{>0}$ *sono in corrispondenza biunivoca.*

DIMOSTRAZIONE. Consideriamo la funzione f da $\mathbb{N}$ a $\mathbb{Z}$ che manda un numero naturale pari $2k$ nella sua metà, ossia in k, e un numero naturale dispari $2k+1$ in $-k-1$. Non è difficile (esercizio !) dimostrare che f è bigettiva e dunque che $\mathbb{N}$ e $\mathbb{Z}$ sono equipotenti.

Costruiamo ora una funzione bigettiva g da $\mathbb{N}$ a $\mathbb{N}^{>0}$. Basta porre, per ogni $n \in \mathbb{N}$, $g(n) = n + 1$.

□

La proposizione appena dimostrata può apparire, da un certo punto di vista, sorprendente; infatti, dato che

$$\mathbb{N}^{>0} \subsetneq \mathbb{N} \subsetneq \mathbb{Z}$$

(il simbolo $\subsetneq$ significa "incluso strettamente") a prima vista, sbagliando, avremmo potuto pensare che non è possibile mettere in corrispondenza biunivoca gli elementi di $\mathbb{N}$ con quelli di $\mathbb{N}^{>0}$ e di $\mathbb{Z}$.

Eppure è forte la nostra intuizione che, se fra due insiemi esiste una corrispondenza biunivoca, questi due insiemi hanno "la stessa cardinalità". L'infinito mette dunque in crisi il concetto di "più grande", o meglio, ci chiede di precisarlo: una cosa è l'inclusione, un'altra la cardinalità.

DEFINIZIONE 8.2. Diciamo che due insiemi X e Y hanno la stessa cardinalità ($|X| = |Y|$), o che sono equipotenti, se esiste una funzione bigettiva $f : X \to Y$. Se esiste una funzione iniettiva da X a Y si dice che X ha cardinalità minore o uguale a quella di Y e si scrive $|X| \leq |Y|$. Scriviamo $|X| < |Y|$ (e diciamo che X ha cardinalità strettamente minore di quella Y) quando vale $|X| \leq |Y|$ e X e Y non sono equipotenti.

Nello studio degli insiemi infiniti procederemo come abbiamo fatto per quelli di cardinalità finita, ossia individueremo alcuni insiemi "campione" che serviranno da confronto e riferimento per gli altri insiemi infiniti.

2. Gli insiemi infiniti numerabili

Il primo insieme "campione" che prendiamo in considerazione è $\mathbb{N}$: diremo che un insieme è "infinito numerabile" se è equipotente a $\mathbb{N}$.

Fra gli insiemi infiniti numerabili, oltre ad $\mathbb{N}$ stesso, abbiamo già individuato $\mathbb{Z}$ e $\mathbb{N}^{>0}$. Quest'ultimo è $\mathbb{N}$ privato di uno dei suoi elementi.

Sorge subito una domanda: cosa accade se ad $\mathbb{N}$ leviamo un numero finito, diciamo $m > 0$, di elementi ? Abbiamo ancora un insieme infinito numerabile. La dimostrazione è analoga a quella della equipotenza di $\mathbb{N}$ e $\mathbb{N}^{>0}$: come primo passo osserviamo che $\mathbb{N}$ privato di m elementi è equipotente a $\mathbb{N} - \{0, 1, 2, 3, 4, \ldots, m-1\}$; ci resta dunque da trovare una funzione bigettiva fra $\mathbb{N}$ e $\mathbb{N} - \{0, 1, 2, 3, 4, \ldots, m-1\}$...

Approfondiamo lo studio dei sottoinsiemi infiniti di $\mathbb{N}$. Possiamo dividerli in due famiglie: quelli che hanno complementare finito (ne abbiamo appena parlato) e quelli che hanno complementare infinito (per esempio l'insieme dei numeri pari, il cui complementare, l'insieme dei numeri dispari, è anch'esso infinito). Per entrambe le famiglie vale comunque

TEOREMA 8.3. *Sia A un sottoinsieme infinito di $\mathbb{N}$; allora A è equipotente a $\mathbb{N}$.*

DIMOSTRAZIONE. Dobbiamo costruire una funzione bigettiva da $\mathbb{N}$ ad A. Un modo per farlo, per esempio, è quello di mandare 0 nell'elemento minimo di A (chiamiamolo a_0: esiste per il principio del minimo); poi mandiamo 1 nell'elemento minimo (che chiameremo a_1) di $A - \{a_0\}$, poi 2 nell'elemento minimo di $A - \{a_0, a_1\}$. E così via... □

Non abbiamo difficoltà a riadattare questo teorema esprimendolo con un enunciato leggermente più generale:

TEOREMA 8.4. *Se U è un sottoinsieme infinito di un insieme infinito numerabile X, allora U è infinito numerabile: $|U| = |X|$.*

Torniamo ora all'osservazione che $\mathbb{Z}$ è numerabile; possiamo esprimerla anche dicendo che l'unione di due copie di $\mathbb{N}$ è ancora numerabile. Più in generale:

TEOREMA 8.5. *Se X è un insieme infinito numerabile e Y è un insieme finito o infinito numerabile, allora $X \cup Y$ è un insieme infinito numerabile.*

DIMOSTRAZIONE. Nel passare da X a $X \cup Y$, gli elementi che aggiungiamo veramente sono quelli di $Y - X$. Dividiamo dunque la dimostrazione in due casi a seconda che $Y - X$ risulti infinito o finito.

Se $Y - X$ è finito (poniamo che abbia $m > 0$ elementi), per mostrare che X è equipotente a $X \cup (Y - X)$ possiamo cominciare con l'osservare che X, essendo infinito numerabile, è equipotente a $\mathbb{N}$ ma è anche equipotente, visto il Teorema 8.3, a $\mathbb{N} - \{0, 1, 2, \ldots, m-1\}$. Esiste dunque una funzione bigettiva da X a $\mathbb{N} - \{0, 1, 2, \ldots, m-1\}$. È facile a questo punto "estenderla" ad una funzione bigettiva da $X \cup (Y - X)$ a $\mathbb{N}$.

Se $Y - X$ è infinito, vuol dire che è infinito numerabile. Infatti siamo necessariamente nel caso in cui Y è infinito numerabile ed esiste dunque una funzione bigettiva da Y a $\mathbb{N}$, che per restrizione ci dà una funzione bigettiva da $Y - X$ ad un sottoinsieme di $\mathbb{N}$. Per il Teorema 8.3, sappiamo che tale sottoinsieme è infinito numerabile. Possiamo allora costruire una funzione bigettiva da $X \cup Y = X \cup (Y - X)$ a $\mathbb{Z}$, nel seguente modo: troviamo una funzione bigettiva da X al sottoinsieme di $\mathbb{Z}$ dato dai numeri non negativi, e una funzione bigettiva da $Y - X$ al sottoinsieme dato dai numeri negativi (tali sottoinsiemi sono equipotenti a $\mathbb{N}$). Dunque $X \cup Y$ è equipotente a $\mathbb{Z}$, che, come sappiamo (Proposizione 8.1) è equipotente a $\mathbb{N}$.

□

3. Un'altra definizione di infinito

Nessuna cardinalità infinita è minore di quella numerabile: questo risultato, che è esposto nel seguente teorema, chiarisce come mai si sceglie $\mathbb{N}$ come primo riferimento per valutare gli insiemi infiniti.

TEOREMA 8.6. *Sia X un insieme infinito. Allora X contiene un sottoinsieme infinito numerabile. Dunque vale*

$$|\,\mathbb{N}\,| \leq |X|$$

DIMOSTRAZIONE. Visto che X è infinito, dunque non vuoto, possiamo scegliere un elemento $x_0 \in X$. Consideriamo poi $X - \{x_0\}$: anche questo insieme non è vuoto, e scegliamo $x_1 \in X - \{x_0\}$. Visto che anche $X - \{x_0, x_1\}$ non è vuoto possiamo scegliere $x_2 \in X - \{x_0, x_1\}$ e così via.. Il sottoinsieme di X i cui elementi sono gli x_i è un sottoinsieme infinito numerabile[1]. □

Il teorema appena dimostrato ci permette di fare una ulteriore importante osservazione:

TEOREMA 8.7. *Sia X un insieme infinito. Allora esiste un sottoinsieme proprio $V \subsetneq X$ equipotente a X.*

DIMOSTRAZIONE. L'enunciato si può dimostrare con un procedimento di "incollamento di funzioni". Sia infatti $\mathcal{N} \subset X$ un sottoinsieme numerabile di X (esiste, come ci garantisce il Teorema 8.6). Scegliamo un elemento $\gamma \in \mathcal{N}$. Nel paragrafo precedente abbiamo mostrato come costruire una funzione bigettiva da $\mathbb{N}$ a $\mathbb{N} - \{0\}$; a partire da questa possiamo immediatamente costruire una funzione bigettiva h da $\mathcal{N}$ a $\mathcal{N} - \{\gamma\}$. Poniamo $V = X - \{\gamma\}$. Possiamo ora ottenere una funzione bigettiva f da X a V nel seguente modo: definiamo $f(x) = x$ per ogni $x \in X - \mathcal{N}$ e $f(z) = h(z)$ per ogni $z \in \mathcal{N}$. La f, in altre parole, si comporta come l'identità su $X - \mathcal{N}$, mentre su $\mathcal{N}$ è definita incollando un'altra funzione, la h, che è bigettiva fra $\mathcal{N}$ e $\mathcal{N} - \{\gamma\}$. □

Questo risultato ci permette di dare una caratterizzazione degli insiemi infiniti[2]:

TEOREMA 8.8. *Un insieme è infinito se e solo se è equipotente ad un suo sottoinsieme proprio.*

DIMOSTRAZIONE. Che un insieme infinito abbia questa proprietà lo abbiamo appena visto col Teorema 8.7; che un insieme finito non goda di questa proprietà lo sappiamo grazie al lemma dei cassetti (che, lo ricordiamo, vale appunto per insiemi finiti). □

4. Numerabilità dell'insieme dei numeri razionali

Continuiamo a passare in rassegna alcuni insiemi infiniti, confrontandoli con l'insieme campione $\mathbb{N}$. Possiamo chiederci per esempio se $\mathbb{N} \times \mathbb{N}$ abbia più elementi di $\mathbb{N}$. La risposta è no, e la possiamo ottenere utilizzando il "primo procedimento diagonale di Cantor":

TEOREMA 8.9 (Cantor, 1874). *Il prodotto cartesiano di due insiemi infiniti numerabili è infinito numerabile.*

[1] Questo procedimento nasconde una induzione...ed è simile a quello del Teorema 8.3. In questo caso l'induzione è "rafforzata", a ben guardare, da qualcosa di più, l'*assioma della scelta numerabile*. Non approfondiremo qui questo tema, convinti che la vostra intuizione consideri ragionevole la dimostrazione appena data.

[2] L'enunciato del Teorema 8.8 fu scelto da Dedekind con *definizione* di insieme infinito.

Dimostrazione. Siano A e B gli insiemi in questione. Dato che entrambi sono in corrispondenza biunivoca con $\mathbb{N}$, si osserva immediatamente che $A \times B$ è in corrispondenza biunivoca con $\mathbb{N} \times \mathbb{N}$. Ci basta dunque dimostrare che $\mathbb{N} \times \mathbb{N}$ è infinito numerabile. Cominciamo col rappresentare il prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ nel modo usuale, ossia come insieme di coppie disposte nel piano (possiamo pensare gli elementi di $\mathbb{N} \times \mathbb{N}$ come i punti di coordinate entrambe intere non negative nel piano cartesiano):

$$\begin{array}{cccccc} \ldots & \ldots & & & \\ (0,3) & \ldots & \ldots & & \\ (0,2) & (1,2) & \ldots & \ldots & \\ (0,1) & (1,1) & (2,1) & \ldots & \\ (0,0) & (1,0) & (2,0) & (3,0) & \ldots \end{array}$$

Ora stabiliamo fra $\mathbb{N} \times \mathbb{N}$ e $\mathbb{N}$ la corrispondenza biunivoca suggerita dalla seguente figura:

$$\begin{array}{ccccc} \ldots & \ldots & & & \\ 9 & \ldots & \ldots & & \\ 5 & 8 & \ldots & \ldots & \\ 2 & 4 & 7 & \ldots & \\ 0 & 1 & 3 & 6 & \ldots \end{array}$$

Possiamo così costruire una funzione bigettiva:

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

che manda $(0,0)$ in 0, $(1,0)$ in 1, $(0,1)$ in 2, $(2,0)$ in 3 e così via, "percorrendo" l'insieme $\mathbb{N} \times \mathbb{N}$ per diagonali che vanno dal basso verso l'alto e verso sinistra.

Possiamo anche descrivere f mediante una formula (questo calcolo viene lasciato per esercizio facoltativo):

$$f((m,n)) = \frac{1}{2}(m+n)(m+n+1) + n$$

□

Una conseguenza molto interessante di questo teorema è che anche i numeri razionali sono numerabili:

Teorema 8.10 (Cantor, 1874). *I numeri razionali sono equipotenti ai numeri naturali:* $|\mathbb{N}| = |\mathbb{Q}|$.

Dimostrazione. Per prima cosa scriviamo i numeri razionali come unione disgiunta di tre sottoinsiemi:

$$\mathbb{Q} = \mathbb{Q}^{<0} \cup \{0\} \cup \mathbb{Q}^{>0}$$

Se dimostriamo che $\mathbb{Q}^{>0}$ è infinito numerabile allora possiamo concludere che $\mathbb{Q}$ è infinito numerabile in base alla seguente argomentazione. Si osserva per prima cosa che $\mathbb{Q}^{<0}$ è equipotente a $\mathbb{Q}^{>0}$ (pensiamo per esempio alla funzione bigettiva che manda ogni numero in $\mathbb{Q}^{>0}$ nel suo opposto, che appartiene a $\mathbb{Q}^{<0}$). Poi si nota che $\mathbb{Q}^{\geq 0}$ si può ottenere facendo l'unione di un insieme infinito numerabile ($\mathbb{Q}^{>0}$) con un insieme finito ($\{0\}$), e dunque, per il Teorema 8.5, sappiamo che $\mathbb{Q}^{\geq 0}$ è un insieme infinito numerabile. Infine si conclude che $\mathbb{Q}$ è infinito numerabile esprimendolo come l'unione di due insiemi infiniti numerabili ($\mathbb{Q}^{\geq 0}$ e $\mathbb{Q}^{<0}$) e usando ancora il Teorema 8.5.

Il punto cruciale da dimostrare è dunque che $\mathbb{Q}^{>0}$ è infinito numerabile. Per questo, per prima cosa costruiamo una funzione iniettiva:

$$g : \mathbb{Q}^{>0} \to \mathbb{N} \times \mathbb{N}$$

Definiamola così: preso $r \in \mathbb{Q}^{>0}$ lo scriviamo come

$$r = \frac{a}{b}$$

dove a e b sono numeri interi positivi primi fra loro (questo concetto sarà discusso nel Capitolo 10, ma già sapete, comunque, cosa vuol dire: chiediamo che l'unico intero positivo divisore comune di a e di b sia 1). Visto che c'è un unico modo di esprimere r come frazione di due numeri interi positivi a e b primi fra loro, la funzione che manda $r \in \mathbb{Q}^{>0}$ nella coppia $(a, b) \in \mathbb{N} \times \mathbb{N}$ è ben definita ed è questa la nostra g.

Si osserva immediatamente che g è iniettiva: se infatti avessimo $g(r) = g(s)$, con $r, s \in \mathbb{Q}$, allora questo significherebbe $g(r) = (a, b) = g(s)$ e dunque per costruzione $r = \frac{a}{b}$ ma anche $s = \frac{a}{b}$, ossia $r = s$.

Osservazione 8.11. Certamente g non è surgettiva (la coppia $(6, 4)$, per esempio, non essendo composta da numeri primi fra loro, non può appartenere all'immagine di g) ma questo non è rilevante per la dimostrazione che stiamo facendo.

Ora, l'iniettività di g ci garantisce che $\mathbb{Q}^{>0}$ ha la stessa cardinalità di $g(\mathbb{Q}^{>0})$. Ma $g(\mathbb{Q}^{>0})$ è un sottoinsieme infinito di $\mathbb{N} \times \mathbb{N}$ e, per il Teorema 8.9, sappiamo che $\mathbb{N} \times \mathbb{N}$ è infinito numerabile. Dunque, per il Teorema 8.4 possiamo concludere che $g(\mathbb{Q}^{>0})$ è infinito numerabile, e allora anche $\mathbb{Q}^{>0}$ è infinito numerabile. □

5. Un insieme infinito non numerabile: i numeri reali

I numeri reali sono un esempio di insieme infinito non numerabile:

Teorema 8.12. *(Cantor, 1874)] I numeri reali hanno cardinalità strettamente maggiore di quella dei numeri naturali:* $|\mathbb{N}| < |\mathbb{R}|$.

Dimostrazione. Visto che $\mathbb{N} \subseteq \mathbb{R}$, vale $|\mathbb{N}| \leq |\mathbb{R}|$. Resta allora da dimostrare che non può valere l'uguale, ossia che i due insiemi non sono equipotenti: $|\mathbb{N}| \neq |\mathbb{R}|$. Questo, data la definizione di equipotenza, equivale a dimostrare che non può esistere una funzione bigettiva da $\mathbb{N}$ a $\mathbb{R}$.

Osserviamo che, se mostriamo che non può esistere una funzione surgettiva da $\mathbb{N}$ a $\mathbb{R}$, in particolare non può esistere una funzione bigettiva, dunque sarà sufficiente mostrare che non può esistere una funzione surgettiva da $\mathbb{N}$ a $\mathbb{R}$.

Osserviamo ancora che, se mostriamo che non può esistere una funzione surgettiva da $\mathbb{N}$ all'intervallo $[0, \frac{1}{2}) \subseteq \mathbb{R}$ (con $[0, \frac{1}{2})$ indichiamo l'intervallo con 0 incluso e $\frac{1}{2}$ escluso), allora non può esistere neppure una funzione surgettiva da $\mathbb{N}$ a $\mathbb{R}$ (infatti se esistesse una funzione surgettiva da $\mathbb{N}$ a $\mathbb{R}$, sarebbe facile modificarla in modo da ottenerne una surgettiva da $\mathbb{N}$ a $[0, \frac{1}{2})$..).

Ci siamo dunque ridotti a dimostrare che non può esistere una funzione surgettiva da $\mathbb{N}$ a $[0, \frac{1}{2})$, e lo dimostriamo per assurdo. Supponiamo che $f : \mathbb{N} \to [0, \frac{1}{2})$ sia surgettiva ed elenchiamo tutti gli elementi dell'immagine $f(\mathbb{N})$, scritti in notazione decimale:

$$f(0) = 0, a_{00}a_{01}a_{02}a_{03}a_{04}a_{05}\ldots$$
$$f(1) = 0, a_{10}a_{11}a_{12}a_{13}a_{14}a_{15}\ldots$$
$$f(2) = 0, a_{20}a_{21}a_{22}a_{23}a_{24}a_{25}\ldots$$

$$f(3) = 0, a_{30}a_{31}a_{32}a_{33}a_{34}a_{35}\dots$$
$$f(4) = 0, a_{40}a_{41}a_{42}a_{43}a_{44}a_{45}\dots$$
$$f(5) = 0, a_{50}a_{51}a_{52}a_{53}a_{54}a_{55}\dots$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

Qui i simboli a_{ij} rappresentano le cifre $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ dello sviluppo decimale, e utilizziamo la convenzione per cui i nostri numeri sono scritti evitando di usare "code" infinite di 9.

La nostra strategia consiste ora nel costruire un numero "cattivo" $b \in [0, \frac{1}{2})$ che di sicuro non sta nella lista delle immagini della f, e dunque non appartiene a $f(\mathbb{N})$. In tal modo troviamo un assurdo, perché avevamo supposto che f fosse surgettiva.

Il numero b viene costruito tenendo presenti le cifre $a_{00}, a_{11}, a_{22}, a_{33}, a_{44}, a_{55}\dots$ che si trovano, nella figura qui sopra, sulla diagonale che parte da a_{00} e va verso destra e in basso (questo viene chiamato "il secondo procedimento diagonale di Cantor").

Precisamente, se indichiamo con

$$b = 0, b_0b_1b_2b_3b_4b_5\dots$$

la scrittura decimale di b, noi scegliamo di porre, per ogni $i = 0, 1, 2, 3, 4, 5, \dots$:

$$b_i = 0 \text{ se } a_{ii} \neq 0$$
$$b_i = 1 \text{ se } a_{ii} = 0$$

Possiamo subito osservare che il numero b non può essere uno dei numeri della lista delle immagini della f: preso infatti un qualunque numero della lista, diciamo $f(m)$ con $m \in \mathbb{N}$, b differisce da esso almeno per una cifra decimale, essendo per costruzione $b_m \neq a_{mm}$. □

6. Alla ricerca di altri infiniti..

Per mostrare che esistono anche cardinalità maggiori di quella del continuo, ossia di quella di $\mathbb{R}$, abbiamo enunciato a lezione il seguente teorema di cui in queste note diamo la dimostrazione (facoltativa, molto consigliata!).

Teorema 8.13. *Per ogni insieme, finito o infinito, X, vale che*

$$|X| < |\mathcal{P}(X)|$$

Osservazione 8.14. Ricordiamo che $\mathcal{P}(X)$ indica l'insieme delle parti di X. In particolare per $\mathbb{R}$ vale $|\,\mathbb{R}\,| < |\mathcal{P}(\mathbb{R})|$.

Dimostrazione. Il caso dell'insieme vuoto è banale: $|\emptyset| = 0 < |\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1$.

Sia dunque X non vuoto. Bisogna innanzitutto costruire una funzione iniettiva da X a $\mathcal{P}(X)$, in modo da poter dire che $|X| \leq |\mathcal{P}(X)|$. Poi concluderemo dimostrando che non può esistere una funzione surgettiva - dunque in particolare bigettiva - da X a $\mathcal{P}(X)$.

Una funzione iniettiva da X a $\mathcal{P}(X)$ è per esempio quella che manda ogni $x \in X$ in $\{x\} \in \mathcal{P}(X)$ ossia ogni elemento x nel suo "singoletto".

Supponiamo ora di avere una funzione $f : X \to \mathcal{P}(X)$. Qualunque sia f, esibiremo un elemento di $\mathcal{P}(X)$, ossia un sottoinsieme di X, che non è nell'immagine di f. Dunque f non è surgettiva e, vista la arbitrarietà nella scelta di f, questo vuol dire che non possono esistere funzioni surgettive da X a $\mathcal{P}(X)$, in particolare neppure funzioni bigettive.

Ecco il sottoinsieme "cattivo":

$$A = \{x \in X \mid x \notin f(x)\}$$

Leggiamo bene chi è A; A è il sottoinsieme di X i cui elementi sono tutti quegli $x \in X$ che hanno la seguente proprietà: $x \notin f(x)$ (ricordiamo che $f(x)$ è un elemento di $\mathcal{P}(X)$ e dunque è a sua volta un sottoinsieme di X, per cui ha senso chiedersi se $x \in f(x)$ o $x \notin f(x)$).

Supponiamo che $A \in Imm\ f$, ossia che esista $a \in X$ tale che $f(a) = A$ e mostriamo che questo conduce ad un assurdo. Basta considerare a (ricordiamo che appartiene a X) e A (ricordiamo che è un sottoinsieme di X), chiedersi se $a \in A$ o $a \notin A$ e scoprire che nessuno dei due casi può accadere.

Infatti se $a \in A$ allora, vista la definizione di A, a è uno di quegli elementi x tali che $x \notin f(x)$. Ossia per a accade che $a \notin f(a)$. Ma $f(a) = A$ e dunque accade che $a \notin A$. Assurdo !

Se invece $a \notin A$ allora, vista la definizione di A, a non è uno di quegli elementi x tali che $x \notin f(x)$. Ossia per a accade che $a \in f(a)$ cioè $a \in A$. Assurdo! □

Possiamo dunque costruire una lista di insiemi infiniti con cardinalità strettamente crescenti:

$$|\,\mathbb{N}\,| < |\,\mathbb{R}\,| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < \cdots$$

A questo punto sorgono alcune domande: cosa si può dire di $|\mathcal{P}(\mathbb{N})|$: lo possiamo aggiungere come un nuovo elemento della lista ? Questi nella lista sono tutti gli infiniti possibili ?

La risposta alla prima domanda è che $|\mathcal{P}(\mathbb{N})|$ appare già nella lista: vale infatti $|\mathcal{P}(\mathbb{N})| = |\,\mathbb{R}\,|$ (per una dimostrazione, vedere gli Esercizi 8.18, 8.19 e 8.20 alla fine del capitolo).

Osserviamo che, siccome per il teorema precedente $|\,\mathbb{N}\,| < |\mathcal{P}(\mathbb{N})|$, avremmo anche potuto seguire questa strada "più generale" per dimostrare che la cardinalità del continuo è strettamente maggiore del numerabile.
Torniamo ora alla nostra lista di insiemi infiniti, che sono tutti costruiti a partire da $\mathbb{N}$ ripetendo l'operazione di prendere l'insieme delle parti:

$$|\,\mathbb{N}\,| < |\mathcal{P}(\mathbb{N})| = |\,\mathbb{R}\,| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < \cdots$$

Resta la nostra seconda domanda: questi sono tutti i possibili insiemi infiniti ? Formuliamo anche una domanda che si pone un obiettivo più modesto: ci sono insiemi infiniti di cardinalità strettamente compresa fra $|\,\mathbb{N}\,|$ e $|\,\mathbb{R}\,|$?

Queste due domande sono in realtà molto famose e sono note come:

Ipotesi del continuo: ogni X sottoinsieme di $\mathbb{R}$ che sia infinito non numerabile ha la stessa cardinalità di $\mathbb{R}$.

Ipotesi generalizzata del continuo: se X è un insieme infinito, la sua cardinalità è una di quelle che appaiono nella lista.

La questione diventa sottile, ed è stata analizzata nei lavori di P. Cohen (1963). Per informazioni potete consultare [] e [].

Terminiamo soffermandoci ancora sull'esempio dei numeri reali. Sappiamo che

$$\mathbb{N} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

e che

$$|\,\mathbb{N}\,| = |\,\mathbb{Q}\,| < |\,\mathbb{R}\,|$$

Introduciamo ora un nuovo sottoinsieme di $\mathbb{R}$ che contiene $\mathbb{Q}$.

DEFINIZIONE 8.15. Un numero reale si dice algebrico se è radice di un polinomio

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$$

dove i coefficienti a_i sono numeri razionali. Se un numero reale non è algebrico allora si dice trascendente.

In altre parole, preso un numero reale a, se si trova un polinomio a coefficienti razionali di cui a è radice, allora a è algebrico. Se un tale polinomio non esiste allora a è trascendente. Notiamo che il fatto che il polinomio della definizione sia monico, ossia inizi con x^n, non è importante. Quello che è importante è che sia a coefficienti razionali (perché non é cosí importante che sia monico ?).

Vale che tutti i numeri razionali sono algebrici, ossia $\mathbb{Q} \subseteq \mathcal{A}$ dove $\mathcal{A}$ è l'insieme dei numeri reali algebrici. Se infatti ho un numero razionale $\frac{m}{n}$ $(n \neq 0)$, tale numero è radice del polinomio a coefficienti razionali $x - \frac{m}{n}$ (o di $nx - m$. . . .a riguardo della domanda fatta poche righe fa. . .).

Ma è algebrico anche il numero $\sqrt{2}$ che noi sappiamo non essere razionale. Infatti $\sqrt{2}$ soddisfa il polinomio a coefficienti razionali (addirittura interi) $x^2 - 2$. Dunque $\mathbb{Q} \subsetneq \mathcal{A}$.

Ma non sarà mica che $\mathcal{A} = \mathbb{R}$, ossia che tutti i numeri reali sono algebrici? La risposta è no. Nel XIX secolo furono trovati da vari matematici (Liouville, Hermite, Lindemann. . .) dei numeri che non sono algebrici: tali numeri si chiamano "trascendenti".

Per esempio Hermite dimostrò nel 1873 che e, la base dei logaritmi naturali, è trascendente, e Lindemann nel 1882 dimostrò che π è trascendente.

Il problema di trovare numeri trascendenti è molto complicato.

Questa complicazione ci può sorprendere: possiamo infatti dimostrare che i numeri trascendenti sono "di più" dei numeri algebrici (e dunque dei numeri razionali). Come fare?

Tutto comincia con la seguente osservazione:

ESERCIZIO 8.16. Dimostrare che $\mathcal{A}$ è infinito numerabile.

SOLUZIONE: [Traccia] I polinomi a coefficienti razionali si possono individuare in base al loro grado, che è un numero naturale, e in base ai loro coefficienti, che sono numeri razionali (insomma appartengono ad un insieme numerabile). Dunque i polinomi a coefficienti razionali sono numerabili. D'altra parte, le radici di un polinomio sono finite.. □

Ora scriviamo $\mathbb{R} = \mathcal{A} \cup \mathcal{T}$, dove $\mathcal{T}$ è l'insieme dei numeri trascendenti: a questo punto, anche se non conoscessimo nemmeno un numero trascendente, potremmo comunque affermare che $\mathcal{T}$ non è vuoto, visto che altrimenti avremmo $\mathbb{R} = \mathcal{A}$ e $\mathbb{R}$ sarebbe numerabile. Inoltre $\mathcal{T}$ non può essere né finito né infinito numerabile (altrimenti $\mathbb{R}$ sarebbe unione di due insiemi dei quali uno è infinito numerabile e l'altro è o finito o infinito numerabile e noi sappiamo che questo implicherebbe che $\mathbb{R}$ è numerabile !).

Dunque $\mathcal{T}$ è infinito e non numerabile; insomma $|\,\mathbb{N}\,| < |\mathcal{T}|$, che si può scrivere anche $|\mathcal{A}| < |\mathcal{T}|$. In questo senso i numeri trascendenti sono "di più" dei numeri algebrici !

Utilizzando infine il risultato dell'esercizio 8.18 possiamo precisare ulteriormente questa osservazione e dimostrare che $\mathcal{T}$ è equipotente a $\mathbb{R}$.

7. Esercizi

Il seguente esercizio mostra che il concetto di "dimensione" e quello di cardinalità sono di natura diversa: infatti, per esempio, la retta $\mathbb{R}$*, il piano* $\mathbb{R}^2$ *e lo spazio a tre dimensioni* $\mathbb{R}^3$ *sono tutti equipotenti...*

Esercizio 8.17. Dimostrare che $\mathbb{R}$ è equipotente a $\mathbb{R}^2$. Dimostrare che, per ogni n intero positivo, $\mathbb{R}$ è equipotente a R^n.

Esercizio 8.18. Dimostrare che se un insieme infinito X è equipotente ad un insieme Y, e se Z è un insieme finito o numerabile, allora anche $X \cup Z$ è equipotente a Y.

Soluzione: [Traccia per la risoluzione] Se X è infinito numerabile lo sappiamo già. Cerchiamo di scrivere una dimostrazione che funzioni per X infinito anche non numerabile. Sia $f : X \to Y$ la corrispondenza biunivoca fra X e Y. Estraiamo da X un insieme infinito numerabile N: allora $f(N)$ è un sottoinsieme infinito numerabile di Y e $X - N$ è equipotente a $Y - f(N)$. Per dimostrare dunque che $X \cup Z$ è equipotente a Y resta da verificare che l'insieme $N \cup (Z - X)$, ossia l'insieme degli elementi che bisogna aggiungere a $X - N$ per ottenere $X \cup Z$, è equipotente a $f(N)$. Ma $N \cup (Z - X)$ è unione di un insieme infinito numerabile (l'insieme N) con un insieme finito o infinito numerabile (l'insieme $Z - X$ infatti è sottoinsieme di Z che è finito o infinito numerabile), dunque è infinito numerabile. Anche $f(N)$ è infinito numerabile..)

□

Esercizio 8.19. Dimostrare che la cardinalità di un insieme infinito non cambia se lo uniamo a un insieme finito o numerabile. Dimostrare che la cardinalità di un insieme infinito non cambia se gli sottraiamo un insieme finito. Cosa può accadere quando sottraiamo un insieme numerabile da un insieme numerabile?

Esercizio 8.20. Dimostrare che l' insieme delle parti di $\mathbb{N}$ ha la cardinalità del continuo:

$$|\mathcal{P}(\mathbb{N})| = |\,\mathbb{R}\,|$$

Soluzione: [Traccia per la risoluzione] Per prima cosa si osserva che $|\,\mathbb{R}\,| = |(0,1)|$: una funzione bigettiva fra questi due insiemi è, per esempio, $g : (0,1) \to \mathbb{R}$, con $g(x) = \tan[\pi(x - \frac{1}{2})]$, la cui inversa $g^{-1} : \mathbb{R} \to (0,1)$ è data da $g^{-1}(x) = (\frac{1}{\pi} \arctan x) + \frac{1}{2}$.

Dobbiamo dunque dimostrare che $|\mathcal{P}(\mathbb{N})| = |(0,1)|$. Per l'esercizio precedente sappiamo che $|\mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{N}) - \{\mathbb{N}\}|$ (la cardinalità non cambia se togliamo un elemento), dunque possiamo ridurci a dimostrare che $|\mathcal{P}(\mathbb{N}) - \{\mathbb{N}\}| = |(0,1)|$.
Scriviamo i numeri reali in $(0,1)$ in base binaria. Avremo dunque delle espressioni di questo tipo:

$$0,0011010111001110000010\ldots$$

Per essere sicuri di rappresentare in modo unico ogni elemento di $(0,1)$ ci mettiamo d'accordo di non accettare code infinite di 1.

Ora costruiamo una mappa $h : \mathcal{P}(\mathbb{N}) - \{\mathbb{N}\} \longrightarrow (0,1)$ che risulterà essere bigettiva. L'idea di base sarebbe questa: dato un sottoinsieme $A \subsetneq \mathbb{N}$, vorremmo porre

$$h(A) = 0, a_0 a_1 a_2 \cdots$$

dove $a_i = 0$ se $i \notin A$ e $a_i = 1$ se $i \in A$. Siamo vicini ad una buona definizione, ma bisogna aggiustare qualcosa. Infatti se A contenesse tutti i numeri da un certo numero fissato M in poi, ossia se $\mathbb{N} - A$ fosse finito, allora $h(A)$ risulterebbe un numero scritto con una coda infinita di 1. Dovremmo riscriverlo nella forma da noi accettata, ossia trasformando tutti

gli 1 della coda in 0 e facendo diventare 1 l'ultimo 0 che appariva nella vecchia scrittura di $h(A)$. Esisterebbe allora un insieme finito $B \subseteq \mathbb{N}$ tale che $h(A) = h(B)$, insomma h non sarebbe iniettiva. Come si può rimediare ? Bisogna trattare separatamente gli insiemi $A \subsetneq \mathbb{N}$ che sono finiti, quelli che sono infiniti ma hanno complementare finito e quelli che sono infiniti e hanno complementare infinito..... $\square$

CAPITOLO 9

Altre strategie per contare

1. Il principio di Inclusione-Esclusione

Dati due insiemi finiti A e B, come possiamo contare quanti elementi ha la loro unione $A \cup B$?

Questa semplice domanda è il primo passo per avvicinarci ad una interessante strategia del contare, il principio di inclusione-esclusione.

Non è difficile trovare una risposta; per trovare la cardinalità di $A \cup B$ contiamo quanti sono gli elementi di A, di B e di $A \cap B$ e poi osserviamo che:

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

Per verificare questa formula, mettiamoci "nei panni" di un elemento $x \in A \cup B$; tale elemento viene contato quando calcoliamo $|A \cup B|$ e dà il suo contributo di $+1$. Controlliamo se dà contributi agli addendi $|A|$, $|B|$, $|A \cap B|$, e qual è il suo contributo complessivo all'espressione che compare a destra.

Se x appartiene ad uno solo dei due insiemi A, B, (diciamo, per fissare le idee, che appartenga ad A ma non a B), x viene contato una volta nell'addendo $|A|$, poi non dà contributo né all'addendo $|B|$ né all'addendo $|A \cap B|$, dunque nel membro di destra viene contato, come volevamo, una volta sola.

Se invece x appartiene ad entrambi gli insiemi A e B, allora x viene contato una volta nell'addendo $|A|$, poi un'altra volta nell'addendo $|B|$ e infine, però con il segno meno, nell'addendo $-|A \cap B|$; in conclusione, come volevamo, il contributo di x al membro di sinistra è uguale a $2 - 1 = 1$.

Esercizio 9.1. Quanti sono gli interi tra 1 e 1000 divisibili per 7 o per 11?

Soluzione: Ce ne sono $\lfloor 1000/7 \rfloor = 142$ divisibili per 7, $\lfloor 1000/11 \rfloor = 90$ divisibili per 11, e $\lfloor 1000/7 \cdot 11 \rfloor = 12$ divisibili sia per 7 che per 11. Quindi in totale: $142 + 90 - 12 = 220$. □

Esercizio 9.2. Quante sono le stringhe binarie di lunghezza 8 che iniziano per 0 o finiscono per 11?

Soluzione: Quelle che cominciano per 0 sono 2^7, quelle che finiscono per 11 sono 2^6, quelle che soddisfano entrambe queste richieste sono 2^5. Dunque la risposta è: $2^7 + 2^6 - 2^5 = 128 + 64 - 32 = 160$. □

Risolto il primo problema che ci eravamo posti, il nostro prossimo passo consiste nel "rilanciare" e passare al caso di tre insiemi, ossia nel chiedersi, dati tre insiemi finiti A, B, C, come possiamo calcolare $|A \cup B \cup C|$ (vedi Figura 1).

Anche in questo caso possiamo seguire la strategia di calcolare $|A|$, $|B|$, $|C|$, $|A \cap B|$, $|A \cap C|$, $|B \cap C|$, $|A \cap B \cap C|$, e poi individuare la formula:

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

La dimostrazione della correttezza di questa formula può essere fatta con la stessa tecnica adottata nel caso dell'unione di due insiemi; consideriamo un elemento $x \in A \cup$

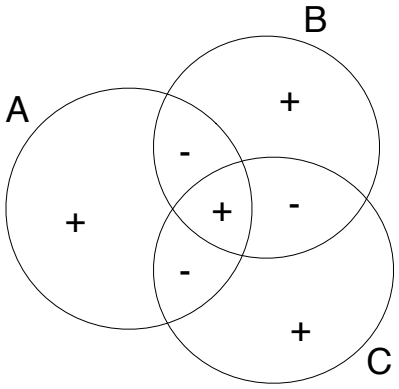

FIGURA 1. Il principio di Inclusione-Esclusione nel caso di tre insiemi. I simboli + e − suggeriscono con quale segno vanno contati gli elementi

$B \cup C$, e distinguiamo i casi: appartiene ad uno solo dei tre insiemi, a due soli di essi o a tutti e tre? In corrispondenza di ciascuno di tali casi, controlliamo se x viene contato, nel membro di destra, nel modo giusto, ossia se complessivamente dà contributo $+1$.

Per esempio, supponiamo che x appartenga solo a due insiemi, diciamo A e B. Allora x viene contato in $|A|$ (col contributo $+1$), in $|B|$ (col contributo $+1$), e in $-|A \cap B|$ (col contributo -1). Visto che un tale x non contribuisce a nessun altro addendo, complessivamente dà contributo $+1$, come volevamo.

E se x appartiene a tutti e tre gli insiemi ? Allora viene contato in $|A|$, in $|B|$, in $|C|$ (per ora siamo al contributo $1+1+1$), poi viene contato in $-|A \cap B|$,$-|A \cap C|$,$-|B \cap C|$ (con contributo $-1-1-1$) e infine in $|A \cap B \cap C|$ (contributo $+1$). Complessivamente il contributo è $3-3+1=1$, anche stavolta in accordo con le nostre attese.

Se completiamo questo ragionamento con la verifica di cosa succede se x appartiene ad uno solo dei tre insiemi (immediata, e lasciata a voi), abbiamo dunque dimostrato la formula:

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

Ci rendiamo conto, a questo punto, di essere pronti a intuire una formula più generale, valida per contare la cardinalità dell'unione di n insiemi A_1,A_2, ..., A_n.

La strategia sarà quella di sommare le cardinalità degli insiemi stessi, di sottrarre le cardinalità di tutte le possibili intersezioni a due a due di tali insiemi, di sommare di nuovo le cardinalità di tutte le possibili intersezioni triple, di sottrarre le cardinalità di tutte le possibili intersezioni quadruple...e così via.

Questa è l'idea del principio di Inclusione-Esclusione...ma come scriverla in maniera soddisfacente?

Avvertiamo il bisogno di introdurre una notazione nuova, che ci permetta di indicare, in maniera compatta, tutte le possibili intersezioni multiple di n insiemi. Eccola, insieme all'enunciato generale del principio di inclusione-esclusione:

TEOREMA 9.3 (Principio di Inclusione-Esclusione). *Consideriamo un intero $n \geq 1$ e siano $A_1, A_2, \ldots, A_n$ insiemi finiti. Dato un sottoinsieme $I = \{i_1, i_2, \ldots, i_r\}$ di $\mathbb{N}_n$ poniamo*

$$A_I = \bigcap_{i \in I} A_i = A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}$$

Allora

$$|\bigcup_{i=1}^{n} A_i| = \sum_{\emptyset \neq I \subseteq \mathbb{N}_n} (-1)^{|I|-1} |A_I|$$

(si noti che l'indice I nella formula varia fra tutti i sottoinsiemi di $\mathbb{N}_n$ escluso l'insieme vuoto)

DIMOSTRAZIONE. La nostra strategia sarà quella di dimostrare che il membro di sinistra e quello di destra forniscono lo stesso numero, ossia la cardinalità di $\bigcup_{i=1}^{n} A_i$.

Mostreremo cioè che ogni elemento $x \in \bigcup_{i=1}^{n} A_i$ è contato esattamente una volta nel membro di sinistra e in quello di destra della formula. Visto che questo è ovvio per il membro di sinistra, studiamo il membro di destra.

Preso dunque un $x \in \bigcup_{i=1}^{n} A_i$, questo apparterrà ad alcuni degli A_i, diciamo che appartenga esattamente a r di essi: $A_{i_1}, A_{i_2}, \cdots, A_{i_r}$.

Allora x nel membro di destra viene contato esattamente con questo coefficiente:

$$r - \binom{r}{2} + \binom{r}{3} - \binom{r}{4} + \cdots + (-1)^{r-1} \binom{r}{r}$$

Infatti nel membro di destra vengono conteggiati col segno "+" gli elementi di tutti gli r insiemi $A_{i_1}, A_{i_2}, \cdots, A_{i_r}$, col segno "−" gli elementi di tutte le loro $\binom{r}{2}$ intersezioni a due a due, col segno più gli elementi di tutte le loro $\binom{r}{3}$ intersezioni a 3 a 3 e così via...

Ma per il Teorema del binomio di Newton noi sappiamo che

$$0 = (1-1)^r = \binom{r}{0} - \binom{r}{1} + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^r \binom{r}{r}$$

da cui, visto che $\binom{r}{0} = 1$ e $\binom{r}{1} = r$,

$$1 = r - \binom{r}{2} + \binom{r}{3} - \binom{r}{4} + \cdots + (-1)^{r-1} \binom{r}{r}$$

Questo permette di concludere che (indipendentemente da quale sia r) il coefficiente con cui viene contato x nel membro di destra è 1, come volevamo. □

2. Applicazioni del principio di Inclusione-Esclusione

Come prima applicazione del principio di Inclusione-Esclusione occupiamoci di funzioni surgettive. Dati due insiemi finiti non vuoti X e Y, chiamiamo $Surj\ (X \to Y)$ l'insieme di tutte le funzioni surgettive che hanno X come dominio e Y come codominio:

$$Surj\ (X \to Y) = \{f \mid f : X \to Y \quad \text{è una funzione surgettiva}\}$$

Il principio di Inclusione-Esclusione ci permetterà di rispondere alla domanda (in generale non semplice): qual è la cardinalità di $Surj\ (X \to Y)$?

La complessità di questo problema cresce enormemente al crescere della cardinalità di Y. Mentre nei casi $|Y| = 1$ e $|Y| = 2$ possiamo facilmente rispondere, nei casi con

$|Y| \geq 3$ l'uso del principio di Inclusione-Esclusione sarà fondamentale per permetterci di "organizzare" il conto.

Cominciamo ad occuparci del caso $|Y| = 1$. Qui c'è una sola funzione da X a Y, quella che manda ogni elemento di X nell'unico elemento di Y, e tale funzione è surgettiva, dunque la cardinalità che cerchiamo è uguale a 1.

Passiamo allora al caso in cui $|Y| = 2$ e poniamo $Y = \{y_1, y_2\}$. Innanzitutto osserviamo che, perché esistano funzioni surgettive da X a Y bisogna che $|X| \geq 2$. Poi notiamo che una funzione surgettiva è individuata univocamente una volta che sappiamo quali sono gli elementi di X che hanno come immagine y_1 (infatti deduciamo subito da questo che gli altri elementi di X avranno come immagine y_2).

Dunque una funzione surgettiva è univocamente individuata da un sottoinsieme di X (quello, appunto, dato dalle controimmagini di y_1), che non deve essere vuoto (deve effettivamente esistere qualche elemento che ha come immagine y_1) e neppure tutto X (altrimenti nessun elemento avrebbe come immagine y_2..).

Quanti sono tali sottoinsiemi? Sappiamo rispondere: sono $2^n - 2$. Anche in questo caso abbiamo saputo contare le funzioni surgettive. Ritroviamo questi nostri primi calcoli come casi particolari del seguente enunciato generale:

Teorema 9.4. *Siano X e Y finiti non vuoti con $|X| = n \geq 1$ e $|Y| = m \geq 1$. Vale:*

$$|Surj\ (X \to Y)| = \sum_{j=0}^{m} \binom{m}{j} (-1)^j (m-j)^n$$

Osservazione 9.5. Come potete verificare, quando $|Y| = 1$ o $|Y| = 2$, la formula precedente conferma i risultati 1 e $2^n - 2$ che abbiamo ottenuto sopra.

Osservazione 9.6. In particolare se $n < m$ come sappiamo $|Surj\ (X \to Y)| = 0$ dunque la formula sopra ci dice:

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

Un modo ben complicato per scrivere 0.....(!!)

Dimostrazione. Sia $X = \{x_1, x_2, \ldots x_n\}$ e $Y = \{y_1, y_2, \ldots y_m\}$. Per ogni $i = 1, 2, \ldots, m$ chiamiamo A_i l'insieme delle funzioni da X a Y la cui immagine non contiene y_i:

$$A_i = \{g \mid g : X \to Y \ \wedge\ y_i \notin \text{Imm } g\}$$

Allora l'insieme delle funzioni non surgettive coincide con $\bigcup_{i=1}^{m} A_i$; se riusciamo a calcolare la cardinalità di questo insieme possiamo facilmente ricavare quella di $Surj\ (X \to Y)$ "per complementare", visto che conosciamo anche la cardinalità (uguale a m^n) dell'insieme $F(X \to Y)$ di tutte le funzioni da X a Y. Infatti

$$Surj\ (X \to Y) = F(X \to Y) - \bigcup_{i=1}^{m} A_i$$

e dunque

$$|Surj\ (X \to Y)| = m^n - |\bigcup_{i=1}^{m} A_i|$$

Ora, per calcolare $|\bigcup_{i=1}^m A_i|$ possiamo usare il principio di Inclusione-Esclusione. Per prima cosa osserviamo che, se $I = \{i_1, i_2, \dots i_j\} \subseteq \{1, 2, \dots m\}$ allora

$$|A_I| = |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}| = (m-j)^n$$

Infatti $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}$ è l'insieme delle funzioni da X a Y che non contengono nella loro immagine né y_{i_1} né $y_{i_2} \dots$ né y_{i_j} e tale insieme è in corrispondenza biunivoca con l'insieme $F(X \to (Y - \{y_{i_1}, \dots y_{i_j}\}))$. Per il principio di Inclusione-Esclusione:

$$|\bigcup_{i=1}^m A_i| = \sum_{\emptyset \neq I \subseteq \mathbb{N}_m} (-1)^{|I|-1} |A_I| = \sum_{j=1}^m \sum_{\substack{I \subseteq \mathbb{N}_m \\ |I| = j}} (-1)^{j-1}(m-j)^n$$

dove l'ultima espressione è stata ottenuta spezzando la sommatoria: abbiamo raggruppato tutti gli $I \subseteq \mathbb{N}_m$ che hanno la stessa cardinalità j e poi sommato su $j = 1, 2, \dots, m$. Ora, gli $I \subseteq \mathbb{N}_m$ che hanno cardinalità j sono $\binom{m}{j}$, dunque possiamo scrivere:

$$= \sum_{j=1}^m \binom{m}{j} (-1)^{j-1}(m-j)^n$$

In conclusione

$$|Surj\ (X \to Y)| = m^n - \sum_{j=1}^m \binom{m}{j} (-1)^{j-1}(m-j)^n$$

Questa formula può essere espressa in maniera più compatta. Infatti:

$$m^n - \sum_{j=1}^m \binom{m}{j} (-1)^{j-1}(m-j)^n = m^n + \sum_{j=1}^m \binom{m}{j} (-1)^{j}(m-j)^n$$

e, visto che $\binom{m}{0} = 1$, possiamo modificare la sommatoria in modo che includa anche il primo addendo m^n:

$$|Surj\ (X \to Y)| = \sum_{j=0}^m \binom{m}{j} (-1)^{j}(m-j)^n$$

□

3. Una prima presentazione del gruppo simmetrico S_n

Consideriamo un insieme X di cardinalità $n \geq 1$. In questo paragrafo studieremo l'insieme $Bij\ (X \to X)$ delle funzioni bigettive da X in sé stesso. Come abbiamo osservato nel Paragrafo 3 di questo capitolo, vale che

$$|Bij\ (X \to X)| = n!$$

Ora osserviamo che se abbiamo due funzioni $f, g \in Bij\ (X \to X)$ allora le funzioni composte $f \circ g$ e $g \circ f$ sono ancora bigettive, dunque appartengono ancora a $Bij\ (X \to X)$ (in generale, come già sappiamo e come vedremo di nuovo fra poco in un esempio, non è affatto detto che $f \circ g = g \circ f$).

Questo ci permette di vedere $Bij\ (X \to X)$ non solo come un insieme, ma come un insieme munito di una OPERAZIONE, appunto la composizione fra funzioni. Questa operazione ha le seguenti caratteristiche:

- per ogni $f, g, h \in Bij\ (X \to X)$ vale $(f \circ g) \circ h = f \circ (g \circ h)$ (proprietà associativa);

- esiste un elemento neutro per $\circ$, ossia una funzione $e : X \to X$ tale che, per ogni $f \in Bij\ (X \to X)$ vale $f \circ e = e \circ f = f$ (più precisamente l'elemento neutro e è la funzione Id_X che manda ogni elemento di X in sé stesso).
- per ogni $f \in Bij\ (X \to X)$ esiste l'inversa rispetto a $\circ$, ossia una funzione $g \in Bij\ (X \to X)$ tale che $f \circ g = g \circ f = Id_X$.

In generale, un insieme munito di una operazione che soddisfa queste proprietà si chiama **gruppo** (rimandiamo al Capitolo 14 per ulteriori approfondimenti sul concetto di gruppo). Dunque $Bij\ (X \to X)$ è un gruppo. Si nota subito che tutto quello che abbiamo detto fin qui non dipende dal particolare insieme X di cardinalità n che abbiamo scelto; decidiamo allora, per fissare le idee e le notazioni, di scegliere $X = \mathbb{N}_n = \{1, 2, 3, \ldots, n\}$.

Definizione. L'insieme $Bij\ (\mathbb{N}_n \to \mathbb{N}_n)$, con l'operazione di composizione fra funzioni, si chiama **gruppo simmetrico su n elementi** e si indica con S_n. Si dice anche che S_n è il gruppo di tutte le **permutazioni** dei numeri 1,2,...,n.

Come si può rappresentare un elemento di S_n, ossia una funzione in $Bij\ (\mathbb{N}_n \to \mathbb{N}_n)$? Un modo potrebbe essere questo; poniamo per esempio $n = 10$, allora col simbolo

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 6 & 7 & 8 & 2 & 1 & 10 & 9 & 5 \end{pmatrix}$$

intendiamo indicare l'elemento $f \in S_n$ che manda ogni numero in quello che sta sotto di lui: per esempio 1 in 3, 2 in 4, 3 in 6, 4 in 7, 5 in 8, 6 in 2..e così via. Un altro modo di rappresentare la stessa funzione è quello "in cicli":

$$f = (1, 3, 6, 2, 4, 7)(5, 8, 10)(9)$$

Questa scrittura va letta così: il primo ciclo ci dice che la f manda 1 in 3 e 3 in 6 e 6 in 2 e 2 in 4 e 4 in 7 e 7 in 1, ossia ogni elemento viene mandato in quello che lo segue tranne l'ultimo, che viene rimandato nel primo (ecco perché si chiamano "cicli"). Il secondo ciclo dice che 5 viene mandato in 8, 8 in 10 e 10 in 5. L'ultimo ciclo dice che 9 viene mandato in sé stesso, ossia viene lasciato fisso dalla f.

Di solito quando un elemento viene lasciato fisso non lo indichiamo, dunque la stessa f di prima la possiamo anche scrivere (quando è chiaro a quale gruppo S_n si riferisce, in questo caso si tratta di S_{10}):

$$f = (1, 3, 6, 2, 4, 7)(5, 8, 10)$$

E per moltiplicare due elementi di S_n espressi in cicli come facciamo ? Per esempio, se $g \in S_n$ è l'elemento:

$$g = (1, 3)(2, 9)$$

quale è la decomposizione in cicli del prodotto $g \circ f$? Scriviamo

$$g \circ f = (1, 3)(2, 9)(1, 3, 6, 2, 4, 7)(5, 8, 10)$$

mettendo accanto le due espressioni. Fare la composizione fra le funzioni significa seguire il "cammino" di un numero, applicandogli i cicli da destra a sinistra. Per esempio il ciclo più a destra manda il 5 in 8, il secondo ciclo lascia l'8 fisso, il terzo e il quarto anche. Dunque $g \circ f$ manda il 5 in 8. Seguiamo adesso l'8. Il ciclo più a destra lo manda in 10, il secondo ciclo lascia fisso il 10, e così anche il terzo e il quarto. Dunque per ora abbiamo trovato:

$$g \circ f = (5, 8, 10.....$$

Continuiamo: il 10 viene mandato in 5 dal ciclo più a destra, e il 5 vene poi lasciato fisso. Dunque abbiamo chiuso il primo ciclo:

$$g \circ f = (5, 8, 10).....$$

Studiamo adesso l'immagine di un altro numero, per esempio il 2 (possiamo partire da uno qualunque diverso da 5,8,10). Otteniamo

$$g \circ f = (5, 8, 10)(2, 4.....$$

Poi seguiamo il 4

$$g \circ f = (5, 8, 10)(2, 4, 7.....$$

Poi il 7, che viene lasciato fisso dal ciclo più a destra, e viene mandato in 1 dal secondo ciclo. Il terzo ciclo lascia fisso l'1 e il quarto manda 1 in 3. Dunque

$$g \circ f = (5, 8, 10)(2, 4, 7, 3.....$$

Continuando così arriviamo a

$$g \circ f = (5, 8, 10)(2, 4, 7, 3, 6, 9)(1) = (5, 8, 10)(2, 4, 7, 3, 6, 9)$$

che è la decomposizione in cicli disgiunti (ossia cicli tali che un numero compare al più in un solo ciclo) che cercavamo.

Facendo i prodotti in questo modo è facile vedere che, per ogni $n \geq 3$, S_n non è un gruppo commutativo; basta prendere $f = (1, 2)$ $g = (1, 3)$ e calcolare

$$g \circ f = (1, 3)(1, 2) = (1, 2, 3)$$

$$f \circ g = (1, 2)(1, 3) = (1, 3, 2)$$

e osservare che $(1, 2, 3)$ è diversa da $(1, 3, 2)$. Notiamo invece che se avessimo due cicli che coinvolgono numeri diversi (insomma se un numero compare in uno dei due cicli non compare nell'altro) tali cicli commuterebbero fra di loro.

Proviamo a contare la cardinalità di alcuni sottoinsiemi del gruppo simmetrico.

Esempio 9.7. In S_{20} quanti sono gli elementi la cui decomposizione in cicli è costituita da 3 cicli di lunghezza 4 e da un ciclo di lunghezza 5 ? Insomma gli elementi la cui decomposizione ha questa struttura: (, , ,)(, , ,)(, , ,)(, , , ,)?

Innanzitutto scegliamo i 4 numeri che vanno nel "primo" ciclo di lunghezza 4: abbiamo $\binom{20}{4}$ scelte. Una volta scelti, come si possono disporre questi 4 numeri ? Si possono disporre in 4! modi diversi, però notiamo che il ciclo (a, b, c, d) rappresenta lo stesso elemento del ciclo (b, c, d, a) e dei cicli (c, d, a, b), (d, a, b, c). Insomma possiamo far "muovere" i numeri circolarmente in un ciclo senza cambiare l'elemento del gruppo che viene rappresentato. Dunque i 4 numeri si possono disporre dentro il ciclo di lunghezza 4 in modo da creare $\frac{4!}{4} = 6$ elementi diversi di S_{20}. Poi con $\binom{16}{4}$ scelte scegliamo i numeri che vanno nel secondo ciclo di lunghezza 4, e con $\binom{12}{4}$ scegliamo quelli che vanno nel terzo ciclo. In $\binom{8}{5}$ scelte possiamo decidere quali numeri vanno nel ciclo di lunghezza 5.

Tenendo conto di quanto detto fin qui, potremmo proporre il numero:

$$\binom{20}{4}\frac{4!}{4}\binom{16}{4}\frac{4!}{4}\binom{12}{4}\frac{4!}{4}\binom{8}{5}\frac{5!}{5}$$

Però questo numero è troppo grande. Abbiamo commesso un errore: quando abbiamo preparato i tre cicli di lunghezza 4, li consideravamo "ordinati" (il "primo", il "secondo",

il "terzo"). In realtà tali cicli commutano fra loro, perché coinvolgono numeri distinti. Per esempio noi abbiamo contato

$$(1,2,3,4)(5,6,7,8)(9,10,11,12)(13,14,15,16,17)$$

e

$$(5,6,7,8)(1,2,3,4)(9,10,11,12)(13,14,15,16,17)$$

come elementi diversi mentre rappresentano lo stesso elemento di S_{20}.

Siccome ci sono 3! modi di disporre in ordine i tre cicli di lunghezza quattro, la soluzione giusta del nostro esercizio è:

$$\frac{1}{3!}\binom{20}{4}\frac{4!}{4}\binom{16}{4}\frac{4!}{4}\binom{12}{4}\frac{4!}{4}\binom{8}{5}\frac{5!}{5}$$

4. Permutazioni senza punti fissi

I seguenti esempi ci mostrano ancora il principio di Inclusione-Esclusione "in azione", applicato al problema della ricerca di permutazioni senza punti fissi:

Esempio 9.8. Dato un numero intero positivo n trovare una formula per contare quante sono le permutazioni in S_n che non hanno punti fissi.

Chiamiamo $NoFix(S_n)$ l'insieme delle permutazioni in S_n che non lasciano fisso nessun numero 1,2,..., n:

$$NoFix(S_n) = \{\sigma \in S_n \mid s(i) \neq i \quad \forall\, i = 1,2,\ldots,n\}$$

Dunque l'esercizio ci chiede di calcolare $|NoFix(S_n)|$. Anche stavolta conteremo per prima cosa la cardinalità del complementare $S_n - NoFix(S_n)$, ossia la cardinalità del sottoinsieme di S_n costituito dagli elementi che lasciano fisso almeno un numero in $\mathbb{N}_n$.

Per ogni $i = 1,2,\ldots,n$ chiamiamo A_i l'insieme degli elementi di S_n che fissano il numero $i \in \mathbb{N}_n$:

$$A_i = \{g \in S_n \mid g(i) = i\}$$

Allora l'insieme degli elementi di S_n che lasciano fisso almeno un numero in $\mathbb{N}_n$ coincide con $\bigcup_{i=1}^n A_i$. Per calcolare $|\bigcup_{i=1}^n A_i|$ possiamo usare il principio di inclusione esclusione.

Cominciamo osservando che se $I = \{i_1, i_2, \ldots i_j\} \subseteq \{1,2,\ldots n\}$ allora

$$|A_I| = |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}| = (n-j)!$$

Infatti $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}$ è l'insieme degli elementi di S_n tali che fra i loro punti fissi ci sono sicuramente $i_1, i_2, \ldots, i_j$, e un tale elemento di S_n è caratterizzato da come agisce sugli altri $n-j$ numeri: dunque $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}$ è in corrispondenza biunivoca con S_{n-j}. Fra l'altro osserviamo che questo, nel caso in cui $j = n$, è in accordo con la convenzione per cui $0! = 1$; infatti in tal caso $A_1 \cap A_2 \cap \cdots \cap A_n$ consiste di un solo elemento, la permutazione identica Id che lascia fissi tutti i numeri di $\mathbb{N}_n$. Per il principio di inclusione esclusione:

$$|\bigcup_{i=1}^n A_i| = \sum_{\emptyset \neq I \subseteq \mathbb{N}_n} (-1)^{|I|-1}|A_I| = \sum_{j=1}^n \sum_{\substack{I \subseteq \mathbb{N}_n \\ |I| = j}} (-1)^{j-1}(n-j)!$$

dove come di consueto abbiamo spezzato la sommatoria in base alla cardinalità degli insiemi I. Ora, gli $I \subseteq \mathbb{N}_n$ che hanno cardinalità j sono $\binom{n}{j}$, dunque abbiamo:

$$= \sum_{j=1}^{n} \binom{n}{j} (-1)^{j-1} (n-j)!$$

In conclusione

$$|NoFix(S_n)| = |S_n| - |\bigcup_{i=1}^{n} A_i|$$

diventa

$$|NoFix(S_n)| = n! - \sum_{j=1}^{n} \binom{n}{j} (-1)^{j-1} (n-j)!$$

che si può esprimere in maniera più compatta come:

$$|NoFix(S_n)| = \sum_{j=0}^{n} \binom{n}{j} (-1)^{j} (n-j)!$$

Questa è la formula che cercavamo; è interessante provare a riscriverla, tenendo conto che $\binom{n}{j}(n-j)! = \frac{n!}{j!}$:

$$|NoFix(S_n)| = \sum_{j=0}^{n} (-1)^j \frac{n!}{j!} = n!(\sum_{j=0}^{n} (-1)^j \frac{1}{j!})$$

che possiamo anche esprimere senza il simbolo di sommatoria come

$$|NoFix(S_n)| = n!(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \cdots + (-1)^n \frac{1}{n!})$$

Esempio 9.9. Quante sono in S_{15} le permutazioni che fissano esattamente 8 numeri?

Costruiamo una permutazione $\sigma \in S_{15}$ che fissa esattamente 8 numeri. Abbiamo $\binom{15}{8}$ modi di scegliere in $\mathbb{N}_{15}$ gli 8 numeri che verranno fissati. Dopodiché vogliamo che la permutazione agisca sui 7 numeri restanti senza lasciarne nessuno fisso. Dunque la risposta è

$$\binom{15}{8} |NoFix(S_7)| = \frac{15!}{8!\ 7!}\ 7!(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \frac{1}{6!} - \frac{1}{7!})$$

5. Esercizi

Esercizio 9.10. Generalizzare il risultato dell'esempio 9.7, ossia calcolare quanti sono in S_n gli elementi che hanno la seguente decomposizione ciclica: c_1 cicli di lunghezza l_1, c_2 cicli di lunghezza l_2,..,c_k cicli di lunghezza l_k (dove $c_1 l_1 + c_2 l_2 + \cdots + c_k l_k = n$.

Esercizio 9.11. Piero mischia un mazzo di 52 carte e dice: "Scommetto che nessuna carta è rimasta nella posizione in cui era all'inizio (ossia la prima carta non è più la prima, la seconda non è più in seconda posizione, la terza etc..)". Giovanni risponde:"E io invece scommetto che hai torto!". Chi dei due, secondo voi, ha più speranza di vincere? La risposta cambia se il mazzo è da 40 carte?

Esercizio 9.12. Una permutazione che mantiene fissi tutti i numeri salvo due, che vengono scambiati tra loro, si chiama *trasposizione*. Una trasposizione si rappresenta dunque con un 2-ciclo (per esempio, $(1,3)$).
Verificare che, in S_9, vale:

$$(1,3,4,7,9) = (1,9) \circ (1,7) \circ (1,4) \circ (1,3)$$

Dimostrare che, in generale, ogni elemento di S_n può essere scritto come composizione di trasposizioni.

Esercizio 9.13. Dimostrare che la scrittura di un elemento di S_n come prodotto di trasposizioni non è unica:
a) fare un esempio di un elemento che si può scrivere in due modi diversi e le trasposizioni coinvolte nelle due scritture non sono le stesse;
b) fare un esempio di un elemento che si può scrivere in due modi diversi e il numero delle le trasposizioni coinvolte nelle due scritture non è lo stesso.

CAPITOLO 10

Identità di Bezout ed equazioni diofantee

1. La divisione euclidea

Come possiamo distribuire 150 penne fra 70 studenti? Daremo ad ognuno $\frac{150}{70} = 2,142857$ penne? Oppure il problema lo dobbiamo affrontare dicendo che possiamo dare 2 penne ad ogni studente e poi avanza un resto di 10 penne? Questo secondo modo è il più adatto: visto che le penne non si possono "spezzare", il problema era relativo ai numeri interi e deve avere risposta in termini di numeri interi. La divisione che abbiamo fatto, con un quoziente intero (70) e un resto intero (10), è un esempio di "divisione euclidea".

TEOREMA 10.1. *(Teorema della divisione euclidea). Dati a, b interi con $b > 0$ esistono, e sono unici, due interi q (quoziente) ed r (resto), con*

$$a = bq + r \tag{1}$$

$$0 \leq r < b \tag{2}$$

OSSERVAZIONE 10.2. Rimarchiamo subito che uno dei punti qualificanti della definizione della divisione euclidea è la richiesta sul resto, ossia che valga $0 \leq r < b$. Per esempio, volendo distribuire 22 penne fra sette studenti, potrei darne 2 per uno e lasciarne avanzare 8:

$$22 = 7 \cdot 2 + 8$$

Oppure potrei darne tre per uno e avere una sola penna come resto:

$$22 = 7 \cdot 3 + 1$$

Solo quest'ultima è la divisione euclidea di 22 per 7. Infatti 1 soddisfa la condizione $0 \leq 1 < 7$ mentre 8 non soddisfa $0 \leq 8 < 7$. Il teorema che abbiamo enunciato, e che stiamo per dimostrare, dice appunto, a riguardo di questo esempio, che fra le scritture

$$22 = 7a + c$$

con a e c numeri interi, ne esiste una e una sola che è la divisione euclidea di 22 per 7.

OSSERVAZIONE 10.3. Facciamo ancora un altro esempio. Se $a = -15$ e $b = 7$, la divisione euclidea di a per b è:

$$-15 = 7(-3) + 6$$

con quoziente $q = -3$ e resto $r = 6$. L'uguaglianza

$$-15 = 7(-2) - 1$$

per quanto vera, non è la divisione euclidea.

DIMOSTRAZIONE DEL TEOREMA. Consideriamo il caso $a \geq 0$ (se $a < 0$ la dimostrazione è analoga). Possiamo utilizzare il principio del minimo. Consideriamo l'insieme

$$Q = \{m \in \mathbb{N} \mid mb \geq a\}$$

Tale insieme è un sottoinsieme di $\mathbb{N}$ non vuoto (visto che $b > 0$ e dunque $b \geq 1$, Q contiene infiniti interi maggiori di a). Per il principio del minimo Q ammette un minimo, appunto, che chiameremo q. Ora, se $qb = a$ abbiamo già trovato la nostra divisione euclidea:

$$a = bq + 0$$

Se invece $qb > a$ allora deve valere $(q-1)b < a$, altrimenti il minimo di Q sarebbe $q-1$ e non q. La differenza $r = a - (q-1)b$ soddisfa $0 < r < b$ e dunque la divisione euclidea che cercavamo è

$$a = (q-1)b + r$$

Il procedimento che abbiamo seguito dimostra in realtà anche l'unicità del quoziente e del resto. Per una qualunque altra scelta del quoziente diversa da q, infatti, si osserva facilmente che il resto ottenuto non soddisferebbe la richiesta $0 \leq r < b$. □

Esempio 10.4. Concretamente, il quoziente può essere calcolato come $\lfloor a/b \rfloor$, dove il simbolo $\lfloor a/b \rfloor$ indica la *parte intera* di a/b, ossia il più grande intero che è $\leq a/b$.

Per esempio: $a = 1781293$, $b = 1481$, $a/b \approx 1202.7637$, $q = 1202 = \lfloor a/b \rfloor$, $r = 1781293 - 1481 \cdot 1202 = 1131$.

Oppure $a = -7856123$, $b = 9812$, $a/b \approx -800.66840$, $q = -801 = \lfloor a/b \rfloor$, $r = -7856123 - 9812 \cdot (-801) = 3289$.

2. Il massimo comun divisore e l'algoritmo di Euclide

Notazione. Ricordiamo che, dati due numeri interi c e d, diciamo che c divide d se esiste un numero intero k tale che $ck = d$. In tal caso scriviamo $c \mid d$.

Definizione 10.5. Siano $a, b \in \mathbb{Z}$, con almeno uno dei due diverso da 0 (questo si può scrivere così: $(a, b) \in \mathbb{Z} \times \mathbb{Z} - \{(0,0)\}$). Allora il "massimo comun(e) divisore" di a e b è l'unico intero positivo d tale che:

- $d|a$ e $d|b$;
- d è più grande di ogni altro divisore comune di a e b: se $c|a$ e $c|b$, allora deve essere $c \leq d$.

Indicheremo il massimo comun divisore di a e b come $MCD(a, b)$ (talvolta, quando è chiaro che stiamo considerando il massimo comun divisore, ometteremo MCD e scriveremo soltanto (a, b)). Se vale che $MCD(a, b) = 1$ diremo che a e b sono *primi tra loro* o *coprimi*.

Osservazione 10.6. La definizione è ben posta. Infatti almeno un divisore comune positivo di a e b esiste sempre (il numero 1) e dunque l'insieme di tutti i divisori comuni positivi è un sottoinsieme di $\mathbb{N}$ non vuoto e finito (si noti a questo proposito che i suoi elementi sono tutti minori o uguali al minimo fra $|a|$ e $|b|$). Allora esiste unico il massimo di tale insieme, che è appunto il $MCD(a, b)$.

Osserviamo subito che:

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

e anche che:

$$MCD(a, a) = MCD(a, 0) = |a|$$

Calcoliamo per esercizio qualche massimo comun divisore:

$MCD(9, 0) = 9$	$MCD(-5, 0) = 5$	$MCD(-8, -12) = 4$
$MCD(9, 54) = 9$	$MCD(-9, 54) = 9$	$MCD(45, 34) = 1$
$MCD(3, 100) = 1$	$MCD(10, 2^8) = 2$	$MCD(-1, 1) = 1$
$MCD(1, 100) = 1$	$MCD(1, 0) = 1$	$MCD(12, -12) = 12$

Da questi esempi risulta che 45 e 34 sono coprimi, come -1 e 1, 3 e 100, 1 e 100, e anche 1 e 0.

Fin dalle scuole medie conoscete un metodo per calcolare il massimo comuni divisore $MCD(a, b)$ di due numeri interi $a \geq 1$ e $b \geq 1$ di cui conoscete la fattorizzazione in prodotto di primi.

Infatti $MCD(a, b)$ è uguale a 1 se non ci sono primi che compaiono in entrambe le fattorizzazioni; se invece ci sono primi che compaiono in entrambe le fattorizzazioni, $MCD(a, b)$ è uguale al prodotto di tali primi, dove ciascuno di essi è preso con l'esponente minimo con cui compare.
Per esempio, se

$$a = 2^5 \cdot 3^4 \quad \text{e} \quad b = 5 \cdot 7 \cdot 17^3$$

allora

$$MCD(a, b) = 1$$

e se invece

$$a = 2^5 \cdot 3^4 \cdot 7^2 \cdot 11^3 \quad \text{e} \quad b = 2^4 \cdot 3^8 \cdot 5 \cdot 7 \cdot 17^3$$

allora

$$MCD(a, b) = 2^4 \cdot 3^4 \cdot 7$$

Dobbiamo fare adesso due importanti precisazioni su questo metodo.

- La prima è che questo metodo è veloce ed efficiente solo se conosciamo già la fattorizzazione in primi dei due numeri. Ma bisogna tenere conto del fatto che in generale il problema di trovare la fattorizzazione in primi di un numero dato è molto difficile (specialmente se il numero è molto grande), e anzi su questa difficoltà si basa uno dei metodi più efficienti di crittografia usato in questi anni, come vedremo più avanti.[1]
- La seconda è che questo metodo funziona perché la fattorizzazione in prodotto di primi di un numero è essenzialmente *unica*. Questa è una proprietà ben nota, ma che in realtà probabilmente non avete mai dimostrato. Noi la dimostreremo fra poche lezioni. Fino a che non la abbiamo dimostrata, dunque, dovete considerare il metodo esposto sopra "in attesa di spiegazione". Alla fine di tutto il percorso avrete una visione più profonda di questo aspetto dell'aritmetica.

Messo dunque per ora da parte il metodo che passa attraverso la fattorizzazione, il nostro obiettivo è quello di discutere un altro metodo per calcolare il massimo comun divisore, l'*algoritmo di Euclide*. Si tratta in realtà di un metodo molto più rapido ed efficiente del precedente e che oltretutto avrà il merito di aprire la strada ad un risultato fondamentale in aritmetica, il Lemma di Bezout.

Cominciamo con ordine, e descriviamo l'algoritmo di Euclide: supponiamo di voler trovare il MCD di due numeri $a, b \in \mathbb{Z}$ non entrambi nulli. Se uno dei due numeri (per esempio a) è 0, allora sappiamo subito dire che $MCD(0, b)$ è uguale al valore assoluto $|b|$ di b.

Occupiamoci dunque del caso in cui entrambi i numeri sono diversi da zero. Se vale per esempio che $|a| \geq |b| > 0$ applichiamo l'algoritmo direttamente al calcolo di $MCD(|a|, |b|)$. Cominciamo con la divisione euclidea di $|a|$ per $|b|$:

$$|a| = |b|q + r_1 \quad \text{con} \quad 0 \leq r_1 < |b|$$

[1] Per dare un'idea della scala di grandezza a cui si riferisce il nostro discorso, anticipiamo fin d'ora che il metodo di crittografia RSA si basa sul fatto che, attualmente, non sia possibile fattorizzare "in tempo utile" un numero di 600 cifre che è il prodotto di due primi.

Se $r_1 = 0$ abbiamo finito, perché possiamo concludere subito che $|b| = MCD(|a|, |b|) = MCD(a, b)$. Altrimenti proseguiamo con delle divisioni euclidee successive finché non si trova un resto uguale a 0:

$$\begin{gathered}
|a| = |b|q + r_1 \quad \text{con} \quad 0 < r_1 < |b| \\
|b| = r_1 \cdot q_1 + r_2 \quad \text{con} \quad 0 < r_2 < r_1 \\
r_1 = r_2 q_2 + r_3 \quad \text{con} \quad 0 < r_3 < r_2 \\
\cdots\cdots\cdots \\
r_{n-2} = r_{n-1} q_{n-1} + r_n \quad \text{con} \quad 0 < r_n < r_{n-1} \\
r_{n-1} = r_n q_n + 0
\end{gathered}$$

A questo punto concludiamo che $r_n = MCD(|a|, |b|) = MCD(a, b)$.

Per dimostrare che il metodo dell'algoritmo funziona, dobbiamo rispondere a due domande.

- Perché l'algoritmo termina sempre entro un numero finito di passi? Perché ad ogni passo otteniamo un resto r_j che è un numero naturale ed è strettamente minore del resto precedente. Se potessimo continuare all'infinito, l'insieme dei resti contraddirebbe il principio del minimo (sarebbe un sottoinsieme di $\mathbb{N}$ non vuoto senza minimo..).

- Perché r_n è proprio il MCD che cercavamo? Il punto cruciale, è dato dal seguente:

  TEOREMA 10.7. *Dati $a, b, c, d \in \mathbb{Z}$ con almeno uno fra a, b non nullo e almeno uno fra b, d non nullo, che soddisfano*

  $$a = bc + d$$

  allora vale che $MCD(a, b) = MCD(b, d)$.

  DIMOSTRAZIONE. La strategia è la seguente: mostreremo che l'insieme $DIV(a, b)$ dei divisori comuni positivi di a e b è uguale all'insieme $DIV(b, d)$ dei divisori comuni positivi di b e d. A quel punto avremo finito, perché $MCD(a, b)$ è il massimo elemento di $DIV(a, b)$ e $MCD(b, d)$ è il massimo elemento di $DIV(b, d)$, ossia...dello stesso insieme.

  Dimostriamo dunque che $DIV(a, b) \subseteq DIV(b, d)$ (l'inclusione opposta si dimostra in maniera analoga). Prendiamo un elemento $\gamma \in DIV(a, b)$. Visto che $\gamma | a$ e $\gamma | b$ allora γ divide anche $a - bc$ ovvero γ divide d. Dunque $\gamma \in DIV(b, d)$, come volevamo dimostrare.

  □

  Applicando questo lemma ai vari passaggi del nostro algoritmo di Euclide otteniamo:

  $$MCD(|a|, |b|) = MCD(|b|, r_1) = MCD(r_1, r_2) = MCD(r_2, r_3) = \ldots$$

  e così via (questo "così via" nasconde una facile induzione!) fino a

  $$\ldots = MCD(r_{n-2}, r_{n-1}) = MCD(r_{n-1}, r_n)$$

  Ma $MCD(r_{n-1}, r_n)$ è proprio r_n, visto che $r_n | r_{n-1}$. Ripercorrendo tutta la catena di uguaglianze scopriamo di aver dimostrato che

  $$MCD(|a|, |b|) = r_n$$

e dunque ora sappiamo perché l'algoritmo di Euclide funziona!

3. Una stima del numero di passi necessario per portare a termine l'algoritmo di Euclide

Come abbiamo anticipato, l'algoritmo di Euclide ha una grande importanza non solo sul piano teorico, ma anche su quello computazionale. Vogliamo allora trovare una stima del numero di passi necessario per terminare l'algoritmo.

Riferiamoci dunque all'algoritmo per trovare il $MCD(|a|,|b|)$ ($|a| \geq |b| \geq 1$) illustrato nel paragrafo precedente. Supponiamo che $a \geq b \geq 1 > 0$, per liberarci dei valori assoluti, che appesantiscono la notazione. Chiamiamo poi $b = r_0$, così da poter affermare che, se il massimo comun divisore risulta essere r_n, abbiamo dovuto fare $n+1$ divisioni euclidee per concludere l'algoritmo. Cerchiamo dunque di stimare il numero di passi $n+1$, in funzione dei dati iniziali (che sono a e b).

Per prima cosa osserviamo che $b = r_0 > 2r_2$, infatti $r_0 = r_1 q_1 + r_2 \geq r_1 + r_2 > r_2 + r_2$.

Allo stesso modo $r_2 > 2r_4$ e così via..., per induzione si mostra che $r_{k-2} > 2r_k$ per ogni $2 \leq k \leq n$. Dunque, se n è pari, $b > 2^{\frac{n}{2}} r_n > 2^{\frac{n}{2}}$. Se invece n è dispari, $b > 2^{\frac{n-1}{2}} r_{n-1} > 2^{\frac{n}{2}}$, visto che $r_{n-1} \geq 2$ (infatti $r_{n-1} > r_n \geq 1$). In entrambi i casi, comunque, possiamo dire che $b > 2^{\frac{n}{2}}$.

Allora $\log_2 b > \frac{n}{2}$, quindi $2\log_2 b > n$, da cui otteniamo

$$n + 1 < 2\log_2 b + 1$$

Questa che abbiamo appena ottenuto è una prima stima.

Il matematico francese Lamé nell'ottocento aveva ottenuto una stima, sempre legata al *logaritmo* di b, ma con una costante migliore. Vediamo come. Cominciamo col chiederci quali sono gli a e b più piccoli che generano un algoritmo di Euclide con $n+1$ divisioni. Se $n = 0$, la risposta è $a = b = 1$; se invece $n > 0$ otterremo gli a e b minimi percorrendo l'algoritmo alla rovescia e chiedendo che r_n, l'ultimo resto non zero, e $q_1, q_2, \ldots, q_{n-1}, q_n$ siano più piccoli possibile.

Quindi partiamo da $r_n = 1$; osserviamo poi che q_n deve essere ≥ 2 visto che $r_{n-1} = r_n q_n$ e $r_{n-1} > r_n$. Dunque il q_n più piccolo possibile è $q_n = 2$ e di conseguenza abbiamo $r_{n-1} = 2$. A questo punto $r_{n-2} = 2q_{n-1} + 1 \geq 2 + 1 = 3$. Continuando a percorrere alla rovescia l'algoritmo, abbiamo $r_{n-3} = r_{n-2}q_{n-2} + r_{n-1} \geq 3q_{n-2} + 2 \geq 3 + 2 = 5$. Al passo successivo otterremo $r_{n-4} \geq 5 + 3 = 8$...e così via. Scegliendo $q_1 = q_2 = \cdots = q_{n-1} = 1$ otteniamo proprio gli r_j minimi, ossia $r_{n-2} = 3$, $r_{n-3} = 5$, $r_{n-4} = 8$...

Sono apparsi i numeri di Fibonacci. !!!!

Nel nostro ragionamento abbiamo ottenuto come resti minimi $r_n = 1 = F_2$, $r_{n-1} = 2 = F_3$, $r_{n-2} = 3 = F_4$, $r_{n-3} = 5 = F_5$ e $r_{n-4} = 8 = F_6$. Come avete capito, si può facilmente dimostrare per induzione che $r_{n-j} \geq F_{j+2}$ e che con le scelte minime possibili di r_n e dei q_j risulta $r_{n-j} = F_{j+2}$.

Dunque b che, nelle nostre notazioni, è r_0, risulta sempre maggiore o uguale a F_{n+2}, e con le scelte minime possibili di r_n e dei q_j risulta esattamente uguale a F_{n+2}.

Inoltre nel caso minimo possibile le informazioni $r_1 = F_{n+1}$ e $b = F_{n+2}$ implicano che $a = F_{n+3}$, ossia, ricapitolando, abbiamo scoperto che l'algoritmo di Euclide per la coppia (F_{n+3}, F_{n+2}) richiede esattamente $n+1$ passi e che fra tutti gli algoritmi di Euclide lunghi $n+1$ passi è 'minimo', in questo senso: se l'algoritmo per la coppia (a, b) ha $n+1$ passi allora vale che $a \geq F_{n+3}$ e $b \geq F_{n+2}$.

Utilizzeremo adesso la formula non ricorsiva per i numeri di Fibonacci data dal Teorema 5.31: per ogni $n \geq 0$ vale

$$F_{n+2} = \frac{\alpha^{n+2} - \beta^{n+2}}{\sqrt{5}},$$

dove $\alpha = \frac{1+\sqrt{5}}{2} \cong 1,618$ e $\beta = \frac{1-\sqrt{5}}{2} \cong -0,618$ sono le due soluzioni dell'equazione $x^2 - x - 1 = 0$. Possiamo usare questa formula per stimare F_{n+2} dimostrando che $F_{n+2} \geq \alpha^n$.

Infatti

$$F_{n+2} = \frac{\alpha^{n+2} - \beta^{n+2}}{\sqrt{5}} \geq \alpha^n$$

equivale a:

$$\alpha^2 - \left(\frac{\beta}{\alpha}\right)^n \beta^2 \geq \sqrt{5}.$$

Per $n = 0$ si tratta di una uguaglianza. Per $n \geq 1$, dai valori approssimati scritti sopra deduciamo che certamente $|\frac{\beta}{\alpha}| < \frac{1}{2}$, quindi, sia che n sia pari sia che sia dispari,

$$\alpha^2 - \left(\frac{\beta}{\alpha}\right)^n \beta^2 > \alpha^2 - \frac{1}{2}\beta^2.$$

Adesso, anche senza sviluppare ulteriormente il calcolo, possiamo verificare direttamente che $\alpha^2 - \frac{1}{2}\beta^2 > \sqrt{5}$ (resistete alla tentazione di usare la calcolatrice, in realtà per questo conto non serve!).

In conclusione abbiamo scoperto che $b \geq F_{n+2} \geq \alpha^n$. Allora, passando ai logaritmi, abbiamo $n \leq \log_\alpha b$ e quindi $n + 1 \leq \log_\alpha b + 1$.

È una stima migliore della precedente; chi vuole ottenerne una senza il logaritmo in base α, può osservare che $log_\alpha b = \frac{1}{\log_b \alpha}$ oppure, a costo di peggiorare un pochino la stima, può utilizzare la disuguaglianza $\log_{10} \alpha > \frac{1}{5}$ (verificatela, stavolta anche con la calcolatrice). Infatti da $n \leq \log_\alpha b$ si ottiene, moltiplicando a sinistra per $\frac{1}{5}$ e a destra per $\log_{10} \alpha$, la nuova disuguaglianza $\frac{n}{5} < \log_{10} \alpha \log_\alpha b = \log_{10} b$, dove abbiamo usato le proprietà elementari del cambio di base nei logaritmi. Riassumiamo questo risultato nell'enunciato del seguente:

Teorema 10.8. *Dato un algoritmo di Euclide per trovare $MCD(a, b)$ con $a \geq b \geq 1$, che richiede $n + 1$ divisioni euclidee, vale*

$$n + 1 < 5 \log_{10} b + 1$$

Questa stima è migliore di quella che avevamo ricavato all'inizio del paragrafo, in cui compare $2 \log_2 b$, perchè $5 \log_{10} b = 5 \log_{10} 2 \log_2 b$, quindi tutto si riduce a controllare se $5 \log_{10} 2 = \log_{10} 2^5$ è minore di 2...e la verifica è immediata.

Dalla stima $n + 1 < 5 \log_{10} b + 1$ se ne può ottenere un'altra in cui entra in gioco il numero delle cifre di b (nella scrittura decimale). Infatti il numero di cifre che si usano per scrivere un numero intero positivo b in base 10 è uguale a $\lfloor \log_{10} b \rfloor + 1$ dove $\lfloor x \rfloor$ indica, come abbiamo già visto, la parte intera di x, insomma il più grande numero intero che è minore o uguale a x.

Allora da $n + 1 < 5 \log_{10} b + 1$ possiamo ottenere

$$n + 1 < 5 \log_{10} b + 1 < 5(\lfloor \log_{10} b \rfloor + 1) + 1$$

Abbiamo insomma, come corollario del Teorema 10.8, ancora una nuova stima:

Corollario 10.9. *Dato un algoritmo di Euclide per trovare $MCD(a, b)$ con $a \geq b \geq 1$, che richiede $n + 1$ divisioni euclidee, vale*

$$n + 1 \leq 5 \; cifre(b)$$

dove $cifre(b)$ indica il numero delle cifre di b scritto in notazione decimale.

4. L'Identità di Bezout

Vogliamo ora mettere in luce una proprietà del massimo comune divisore che giocherà un ruolo fondamentale in tutta la nostra introduzione all'aritmetica: il massimo comun divisore di due numeri a e b è il più piccolo intero positivo che può essere ottenuto quando consideriamo le espressioni del tipo $ax + by$ al variare di x e y fra i numeri interi.

TEOREMA 10.10 (Identità di Bezout o Lemma di Bezout[2]). *Dati due numeri interi a e b con $(a, b) \neq (0, 0)$, esistono due numeri interi m e n tali che*

$$MCD(a, b) = am + bn$$

Si dice che $MCD(a, b)$ può essere espresso come combinazione lineare a coefficienti interi di a e di b.

OSSERVAZIONE 10.11. Il teorema dice che esistono m ed n tali che $MCD(a, b) = am + bn$, ma non dice che sono unici. Infatti, come risulterà dalla teoria delle equazioni diofantee lineari, ci sono infinite scelte possibili di una coppia (m, n) tale che $MCD(a, b) = am + bn$.

DIMOSTRAZIONE. Consideriamo l'insieme $CL^+(a, b)$ di tutte le possibili combinazioni lineari **positive** a coefficienti interi di a e b, ossia

$$CL^+(a, b) = \{ar + bs \mid r \in \mathbb{Z},\ s \in \mathbb{Z},\ ar + bs > 0\}$$

Tale insieme è non vuoto. Infatti supponiamo che $a \neq 0$ (altrimenti si fa lo stesso ragionamento con b). Allora si trovano degli elementi dell'insieme $CL^+(a, b)$ per esempio scegliendo $s = 0$ e r tale che $ra > 0$. Già così abbiamo esibito infiniti elementi nell'insieme $CL^+(a, b)$.

Inoltre $CL^+(a, b) \subseteq \mathbb{N}$. Dunque, per il principio del buon ordinamento, $CL^+(a, b)$ ammette minimo.

Sia d tale minimo: in particolare, dato che $d \in CL^+(a, b)$, esistono un $m \in \mathbb{Z}$ ed un $n \in \mathbb{Z}$ tali che

$$d = am + bn$$

La dimostrazione del teorema si conclude ora mostrando che $d = MCD(a, b)$. Infatti d soddisfa le proprietà del massimo comune divisore, ossia:

- $d|a$ e $d|b$
- se $c|a$ e $c|b$ allora $c \leq d$

Per il primo punto, facciamo la divisione euclidea fra a e d. Sarà $a = qd + r$ con $0 \leq r < d$.

Allora

$$a = q(am + bn) + r$$

da cui

$$r = (-qm + 1)a + (-qn)b$$

Ma allora r si esprime come combinazione lineare a coefficienti interi di a e di b. Se fosse $r > 0$ avremmo che $r \in CL^+(a, b)$ per definizione di $CL^+(a, b)$. Questo non può succedere perché $0 \leq r < d$ e d era stato scelto come **minimo** elemento di $CL^+(a, b)$.

Dunque deve essere $r = 0$. Questo vuol dire che $a = qd + 0$, ossia che $d|a$. Allo stesso modo si dimostra che $d|b$.

Il secondo punto è immediato. Infatti se $c|a$ e $c|b$ allora $c|am+bn$ cioè $c|d$, in particolare $c \leq d$.

[2]Prende il nome dal matematico francese Etienne Bezout, 1730-1783.

□

COROLLARIO 10.12. *Dati due numeri interi a e b con $(a,b) \neq (0,0)$, se $c|a$ e $c|b$, allora non solo $c \leq MCD(a,b)$ ma più precisamente vale che $c|MCD(a,b)$.*

Riguardando la dimostrazione del teorema, ci accorgiamo che abbiamo dimostrato il risultato annunciato all'inizio del paragrafo (che è un po' più forte di quello nell'enunciato del teorema):

TEOREMA 10.13. *Dati due numeri interi a e b con $(a,b) \neq (0,0)$, $MCD(a,b)$ è il più piccolo numero intero positivo ottenibile come combinazione lineare intera di a e di b.*

Sottolineiamo che se dividiamo due numeri per il loro massimo comun divisore, i due quozienti ottenuti sono primi fra loro:

COROLLARIO 10.14. *Presi due numeri interi a e b non entrambi nulli, se li dividiamo per il loro massimo comun divisore $MCD(a,b)$ otteniamo due numeri*

$$a' = \frac{a}{MCD(a,b)} \qquad b' = \frac{b}{MCD(a,b)}$$

che sono primi fra loro.

DIMOSTRAZIONE. Si può vedere in due modi, entrambi molto semplici. Il primo modo è il seguente: se ci fosse un divisore comune $d > 1$ di a' e b', allora $d \cdot MCD(a,b)$ dividerebbe sia a sia b e sarebbe più grande di $MCD(a,b)$, assurdo.

Il secondo parte dall'identità di Bezout

$$MCD(a,b) = am + bn$$

Dividendo per $MCD(a,b)$ si ottiene

$$1 = a'm + b'n$$

e dunque 1 è il più piccolo numero intero positivo ottenibile come combinazione lineare intera di a' e di b'.

□

Concludiamo con una osservazione aritmetica importante, nella cui dimostrazione l'Identità di Bezout gioca un ruolo fondamentale:

TEOREMA 10.15. *Siano $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $MCD(a,b) = 1$ allora $a \mid c$.*

DIMOSTRAZIONE. Visto che $MCD(a,b) = 1$ allora per l'Identità di Bezout possiamo trovare $m, n \in \mathbb{Z}$ tali che

$$1 = an + bm$$

Moltiplicando entrambi i membri per c otteniamo:

$$c = acn + bcm$$

Questo ci permette di concludere che $a \mid c$. Infatti $a \mid acn$ (ovviamente) e $a \mid bcm$ (visto che $a \mid bc$ per ipotesi), dunque a divide la somma $acn + bcm$ che è uguale a c.

□

OSSERVAZIONE 10.16. La dimostrazione precedente è breve ma non è banale. **Il Teorema 10.15 è alla base del fatto che la fattorizzazione in prodotto di primi di un numero intero è unica**, come vedremo in seguito.

5. Un metodo costruttivo per ottenere l'Identità di Bezout

Dati due numeri interi non entrambi nulli a e b, l'Identità di Bezout, come abbiamo visto nel Paragrafo 4, ci dice che è possibile trovare due numeri interi m e n tali che

$$MCD(a, b) = am + bn$$

Ma la dimostrazione che abbiamo proposto in quel paragrafo non ci dà un metodo concreto per trovare un m e un n che soddisfino l'uguaglianza scritta sopra. In questo paragrafo colmeremo questa lacuna, descrivendo un metodo che si basa sull'algoritmo di Euclide, utilizzato due volte, nel modo usuale e "a rovescio".

Prendiamo per esempio $a = 1020$ e $b = 351$ e calcoliamo $MCD(a, b)$ tramite l'algoritmo di Euclide:

$$\begin{aligned}
1020 &= 351 \cdot 2 + 318 \\
351 &= 318 \cdot 1 + 33 \\
318 &= 33 \cdot 9 + 21 \\
33 &= 21 \cdot 1 + 12 \\
21 &= 12 \cdot 1 + 9 \\
12 &= 9 \cdot 1 + 3 \\
9 &= 3 \cdot 3 + 0
\end{aligned}$$

Dunque abbiamo trovato che $MCD(1020, 351) = 3$. Scriviamo adesso di nuovo tutte le equazioni dell'algoritmo (tranne l'ultima) ponendo a sinistra i resti:

$$\begin{aligned}
318 &= 1020 - 351 \cdot 2 \\
33 &= 351 - 318 \cdot 1 \\
21 &= 318 - 33 \cdot 9 \\
12 &= 33 - 21 \cdot 1 \\
9 &= 21 - 12 \cdot 1 \\
3 &= 12 - 9 \cdot 1
\end{aligned}$$

Ora ripercorriamo l'algoritmo "a rovescio": cominciamo da $3 = 12 - 9 \cdot 1$. Ricordiamo che come obiettivo finale vogliamo trasformare questa equazione in una del tipo

$$3 = 1020m + 351n$$

Cominciamo utilizzando l'equazione $9 = 21 - 12 \cdot 1$. Possiamo usarla per sostituire il 9 ed ottenere 3 espresso come combinazione lineare di 12 e di 21:

$$3 = 12 - 9 \cdot 1 = 12 - (21 - 12 \cdot 1) \cdot 1 = 12 \cdot 2 - 21$$

A questo punto facciamo entrare in gioco l'equazione $12 = 33 - 21 \cdot 1$. La utilizziamo per sostituire il 12 ed ottenere 3 come combinazione lineare di 33 e di 21:

$$3 = 12 \cdot 2 - 21 = (33 - 21 \cdot 1) \cdot 2 - 21 = 33 \cdot 2 - 21 \cdot 3$$

Continuando,

$$3 = 33 \cdot 2 - 21 \cdot 3 = 33 \cdot 2 - (318 - 33 \cdot 9) \cdot 3 = 33 \cdot 29 - 318 \cdot 3 =$$

$$= 33 \cdot 29 - 318 \cdot 3 = (351 - 318 \cdot 1) \cdot 29 - 318 \cdot 3 = 351 \cdot 29 - 318 \cdot 32$$

Infine, chiamando in causa $318 = 1020 - 351 \cdot 2$:

$$3 = 351 \cdot 29 - 318 \cdot 32 = 351 \cdot 29 - (1020 - 351 \cdot 2) \cdot 32 = 1020(-32) + 351 \cdot 93$$

Abbiamo dunque trovato $m = -32$ e $n = 93$:

$$3 = 1020(-32) + 351 \cdot 93$$

Osservazione 10.17. Come abbiamo già preannunciato, quando parleremo di equazioni diofantee mostreremo che questa è solo una delle infinite possibili coppie (m, n) che soddisfano l'identità di Bezout

$$3 = 1020m + 351n$$

Anche se si tratta solo di un esempio, non è difficile intuire che il metodo funziona sempre, per ogni a e b di cui è possibile calcolare il massimo comun divisore. Questa è dunque un'altra possibile via di dimostrazione dell'identità di Bezout (radicalmente diversa dall'altra, che era "esistenziale": questa la potremmo chiamare "costruttiva", visto che fornisce un algoritmo concreto per trovare i numeri m e n).

Lasciamo per esercizio (vedi Esercizio 10.24) i dettagli di questa dimostrazione (che può essere svolta per induzione sul numero di passi che occorrono per concludere l'algoritmo di Euclide).

Un metodo "compatto" per organizzare il calcolo viene illustrato nell'esempio seguente:

Esempio 10.18. Calcolare $MCD(252, 198)$ e trovare x, y interi tali che $MCD(252, 198) = 252x + 198y$.

Per prima cosa calcoliamo $MCD(252, 198)$.

$$\begin{gathered} 252 = 198 \cdot 1 + 54 \\ 198 = 54 \cdot 3 + 36 \\ 54 = 36 \cdot 1 + 18 \\ 36 = 18 \cdot 2 + 0 \end{gathered}$$

Dunque $MCD(252, 198) = 18$. Scriviamo ora:

$$\begin{array}{rcccccc} & & 252 & = & 252 \cdot \boxed{1} & + & 198 \cdot \boxed{0} \\ & & 198 & = & 252 \cdot \boxed{0} & + & 198 \cdot \boxed{1} \\ 252 - 198 & = & 54 & = & 252 \cdot \boxed{1} & + & 198 \cdot \boxed{(-1)} \\ 198 - 54 \cdot 3 & = & 36 & = & 252 \cdot \boxed{(-3)} & + & 198 \cdot \boxed{4} \\ 54 - 36 & = & 18 & = & 252 \cdot \boxed{4} & + & 198 \cdot \boxed{(-5)} \end{array}$$

Nella colonna centrale abbiamo scritto (dall'alto) 252, 198 e poi i resti ottenuti con l'algoritmo di Euclide. Di ognuno di questi numeri, nella colonna di destra è indicato come si può ottenere come combinazione di 252 e 198[3]. Dunque il risultato finale si legge dall'ultima riga ed è $x = 4, y = -5$.

6. Le equazioni diofantee

Una equazione del tipo

$$ax + by = c$$

dove a, b, c sono numeri interi e x, y sono le variabili, si chiama equazione diofantea.[4]

Risolverla vuol dire trovare una coppia di numeri interi $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ tali che

$$a\overline{x} + b\overline{y} = c$$

[3]Per passare dalla combinazione della terza riga a quella della quarta, per esempio, visto che $36 = 198 - 54 \cdot 3$, abbiamo sommato la combinazione della seconda riga a quella della terza moltiplicata per -3. Questo si traduce in modo rapido facendo la corrispondente operazione sui numeri incorniciati

[4]Il nome deriva da Diofanto di Alessandria, III-IV secolo d.C.

In questo paragrafo studieremo un criterio per decidere se una equazione diofantea ammette soluzione e, nel caso in cui la ammetta, descriveremo un metodo per trovare tutte le sue soluzioni.

Per prima cosa studiamo a parte il caso in cui $a = 0, b = 0$. L'equazione

$$0x + 0y = c$$

ha soluzione se e solo se anche $c = 0$ e in tal caso le sue soluzioni sono infinite, precisamente tutte le possibili coppie $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$.

Rimane da studiare il caso in cui a e b siano non siano entrambi nulli.

Teorema 10.19. *L'equazione diofantea*

$$ax + by = c \tag{10.1}$$

(con a e b non entrambi nulli) ha soluzione se e solo se $MCD(a, b)$ divide c.

Dimostrazione. Viene in nostro aiuto l'Identità di Bezout. Il Teorema 10.10 ci dice infatti che certamente l'equazione diofantea

$$ax + by = MCD(a, b) \tag{10.2}$$

ammette soluzione.

Ma l'equazione che dobbiamo risolvere differisce da questa perché nel membro di destra c'è c invece di $MCD(a, b)$.

Allora tutta la nostra strategia si gioca su questa domanda: $MCD(a, b)$ divide o non divide il numero c?

Se la risposta è sì, ossia $c = MCD(a, b)\ k$ per un certo numero intero k, allora l'equazione (10.1) ammette soluzione. Infatti si parte da una coppia di numeri interi (m, n) che risolve l'equazione (10.2):

$$am + bn = MCD(a, b)$$

e si moltiplicano entrambi i membri per k. Troviamo allora:

$$a(mk) + b(nk) = MCD(a, b) \cdot k = c$$

dunque, (mk, nk) è una soluzione dell'equazione (10.1).

Viceversa, se la risposta è no, ossia $MCD(a, b)$ non divide c, allora l'equazione (10.1) non può avere soluzione e lo possiamo dimostrare per assurdo. Se infatti ammettesse una soluzione (chiamiamola $(\overline{x}, \overline{y})$) considerando l'uguaglianza

$$a\overline{x} + b\overline{y} = c$$

ricaveremmo che, visto che $MCD(a, b)$ divide il membro di sinistra (essendo un divisore sia di a che di b), allora $MCD(a, b)$ deve dividere il membro di destra, ossia c. Questo è assurdo perché eravamo proprio nel caso in cui $MCD(a, b)$ non divide c.

□

Studiamo meglio il caso in cui l'equazione diofantea (10.1) ha soluzione. In questo caso la soluzione sarà una sola o possiamo trovarne più di una?

Per rispondere, prendiamo in considerazione un'altra equazione, "più semplice" della (10.1):

$$ax + by = 0$$

Come vedete, abbiamo sostituito c con 0. Questa si chiama *l'equazione omogenea associata* alla (10.1).

La sua importanza è legata a questa osservazione: se $(\overline{x}, \overline{y})$ è una soluzione di (10.1) e (γ, δ) è una soluzione della equazione omogenea associata, allora $(\overline{x} + \gamma, \overline{y} + \delta)$ è ancora

una soluzione di (10.1). Lo potete subito verificare sommando membro a membro le due uguaglianze:

$$a\overline{x} + b\overline{y} = c$$

$$a\gamma + b\delta = 0$$

Abbiamo trovato un modo per generare altre soluzioni di (10.1), a partire da una soluzione $(\overline{x}, \overline{y})$ data. Ma quante sono le soluzioni della equazione omogenea associata? Troviamole: riscriviamo

$$ax + by = 0$$

come

$$ax = -by$$

Possiamo dividere entrambi i membri per $MCD(a, b)$:

$$\frac{a}{MCD(a,b)}\ x = -\frac{b}{MCD(a,b)}\ y$$

Questa equazione è equivalente a quella iniziale. Supponiamo di avere una soluzione (γ, δ):

$$\frac{a}{MCD(a,b)}\ \gamma = -\frac{b}{MCD(a,b)}\ \delta$$

A questo punto, visto che i due numeri $\dfrac{a}{MCD(a,b)}$ e $\dfrac{b}{MCD(a,b)}$ sono primi fra loro (vedi il Corollario 10.14), il Teorema 10.15 ci dice che $\dfrac{a}{MCD(a,b)}$ deve dividere δ. Allora δ è della forma $\dfrac{a}{MCD(a,b)}\ t$ e γ risulta uguale a $-\dfrac{b}{MCD(a,b)}\ t$.

Viceversa si nota subito che una qualunque coppia della forma

$$(-\frac{b}{MCD(a,b)}\ t, \frac{a}{MCD(a,b)}\ t)$$

con $t \in \mathbb{Z}$ è una soluzione della equazione omogenea associata. Abbiamo dunque trovato TUTTE le soluzioni della equazione omogenea associata, e notiamo che sono infinite!

Saranno dunque infinite anche le soluzioni della equazione diofantea iniziale (10.1). Il seguente teorema afferma che, con le argomentazioni appena esposte, abbiamo in realtà trovato tutte le soluzioni di (10.1):

Teorema 10.20. *Se l'equazione diofantea (10.1) ammette soluzione, allora ammette infinite soluzioni. Presa una soluzione particolare $(\overline{x}, \overline{y})$, l'insieme $\mathcal{S}$ di tutte le soluzioni può essere descritto così:*

$$\mathcal{S} = \{(\overline{x} + \gamma, \overline{y} + \delta) \mid (\gamma, \delta) \ \textit{è soluzione dell'equazione omogenea associata}\}$$

Dimostrazione. Le argomentazioni esposte poco sopra dimostrano che

$$\{(\overline{x} + \gamma, \overline{y} + \delta) \mid (\gamma, \delta) \ \text{è soluzione dell'equazione omogenea associata}\} \subseteq \mathcal{S}$$

Resta da dimostrare l'inclusione opposta, ossia che ogni soluzione di (10.1) è della forma "$(\overline{x}, \overline{y})$ + una soluzione dell'equazione omogenea associata".

Questo segue osservando che, se (α, β) è una soluzione di (10.1), allora $(\alpha - \overline{x}, \beta - \overline{y})$ è una soluzione della equazione omogenea associata.

□

7. Esempio di risoluzione di una equazione diofantea

Troviamo tutte le soluzioni dell'equazione diofantea

$$435x + 102y = 15$$

Ricordiamo che una soluzione è una coppia $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ che soddisfa l'equazione data:

$$435\overline{x} + 102\overline{y} = 15$$

- Per prima cosa verifichiamo se l'equazione proposta ammette soluzioni: sappiamo che questo accade se e solo se $MCD(435, 102) \mid 15$. Usiamo dunque l'algoritmo di Euclide per calcolare $MCD(435, 102)$.

$$435 = 102 \cdot 4 + 27$$

$$102 = 27 \cdot 3 + 21$$

$$27 = 21 \cdot 1 + 6$$

$$21 = 6 \cdot 3 + 3$$

$$6 = 3 \cdot 2 + 0$$

  Dunque $MCD(435, 102) = 3 \mid 15$ e la nostra equazione ammette soluzioni.
- Adesso troviamo una soluzione particolare dell'equazione. Se utilizziamo l'algoritmo di Euclide "alla rovescia" troviamo dopo qualche calcolo che

$$3 = 102 \cdot 64 - 435 \cdot 15$$

  Se moltiplichiamo questa uguaglianza per $\dfrac{15}{MCD(435, 102)} = 5$ otteniamo

$$15 = 102 \cdot 320 - 435 \cdot 75$$

  Abbiamo dunque che $(-75, 320)$ è una soluzione particolare di

$$435x + 102y = 15$$

  È possibile anche seguire una strada leggermente diversa: visto che abbiamo scoperto che $MCD(435, 102) = 3 \mid 15$, osserviamo che l'equazione

$$435x + 102y = 15$$

  è equivalente (ossia ha le stesse soluzioni) di quella che si ottiene dividendo tutti i coefficienti per 3:

$$145x + 34y = 5$$

  Dall'algoritmo di Euclide che abbiamo usato per calcolare $MCD(435, 102)$ possiamo ricavare, dividendo per 3 tutti i dividendi, i divisori e i resti, un algoritmo di Euclide che calcola $MCD(145, 34) = 1$. Ripercorrendo "alla rovescia" questo algoritmo si trova che

$$1 = 34 \cdot 64 - 145 \cdot 15$$

  Se moltiplichiamo questa uguaglianza per 5 otteniamo

$$5 = 34 \cdot 320 - 145 \cdot 75$$

  da cui ricaviamo che $(-75, 320)$ è una soluzione particolare di

$$145x + 34y = 5$$

  Potete scegliere voi fra le due strade illustrate quella che vi sembra più conveniente (in questa seconda i calcoli coinvolgono numeri più piccoli).

- Troviamo adesso tutte le infinite soluzioni della equazione diofantea data. Consideriamo la omogenea associata

$$435x + 102y = 0$$

e calcoliamone tutte le soluzioni. Dividendo entrambi i membri per $3 = MCD(435, 102)$ (IMPORTANTE: ricordarsi sempre di dividere per il MCD a questo punto dello svolgimento!) ci riduciamo a

$$145x + 34y = 0$$

OSSERVAZIONE 10.21. Ovviamente se avete scelto di seguire la strada di studiare invece che

$$435x + 102y = 15$$

l'equazione equivalente

$$145x + 34y = 5$$

avete subito che l'equazione omogenea associata è

$$145x + 34y = 0$$

Dobbiamo dunque trovare tutte le soluzioni di

$$145x = -34y$$

Sappiamo che 145 e 34 sono coprimi, e dunque se $(\overline{x}, \overline{y})$ è una soluzione deve valere $\overline{y} = 145q$, con $q \in \mathbb{Z}$. Sostituendo

$$145\overline{x} = -34 \cdot 145q$$

da cui ricaviamo $\overline{x} = -34q$. Dunque tutte le soluzioni di

$$145x + 34y = 0$$

devono essere della forma $(-34q, 145q)$ con $q \in \mathbb{Z}$. Il Teorema 10.20 ci permette a questo punto di concludere l'esercizio: le soluzioni di

$$145x + 34y = 0$$

sono tutte e sole le coppie $(-34q, 145q)$ al variare di $q \in \mathbb{Z}$ e l'insieme di tutte le soluzioni di

$$435x + 102y = 15$$

è

$$\{(-75 - 34q, 320 + 145q) \mid q \in \mathbb{Z}\}$$

Trovate altri esempi ed esercizi nel libro [**?**], Capitolo 4, Paragrafo 5, pag. 61.

8. Esercizi

ESERCIZIO 10.22. Calcolare i seguenti massimi comuni divisori:

$$MCD(1094, 189) \qquad MCD(2562, 696)$$

Trovare dei numeri interi m, n, s, t tali che:

$$MCD(1094, 189) = 1094m + 189n \qquad MCD(2562, 696) = 2562s + 696t$$

ESERCIZIO 10.23. Trovare due interi a e b tali che l'algoritmo di Euclide per determinare $MCD(a, b)$ consista di esattamente 7 passaggi.

Esercizio 10.24. Dimostrare 'in maniera costruttiva' l'Identità di Bezout, per induzione sul numero di passi dell'algoritmo di Euclide per $MCD(a, b)$.

Esercizio 10.25. Consideriamo la successione dei numeri di Fibonacci F_n ($n \in \mathbb{N}$): Dimostrare che il massimo comun divisore di due numeri di Fibonacci consecutivi è sempre 1.

Esercizio 10.26. Consideriamo l'insieme:

$$A = \{3k \mid k = 1, 2, \ldots, 100\} \cup \{2, 4, 5\}$$

a) Quante sono le funzioni $f : A \to A$?
b) Esistono funzioni $f : A \to A$ tali che, $\forall x \in A$, $MCD(x, f(x)) = 1$?
c) Quante sono le funzioni $f : A \to A$ tali che, $\forall x \in A$, $MCD(x, f(x)) > 1$?
d) Fra le funzioni del punto c), ne esiste almeno una bigettiva diversa dall'identità ?

Esercizio 10.27. Dire se la funzione $f : \mathbb{N}^{>0} \times \mathbb{N}^{>0} \to \mathbb{N}^{>0}$ data da $f(x, y) = x^{MCD(x,y)}$ è iniettiva, surgettiva, bigettiva.
Dire se la funzione $g : \mathbb{N}^{>0} \times \mathbb{N}^{>0} \to \mathbb{N}^{>0} \times \mathbb{N}^{>0}$ data da $f(x, y) = (x \cdot MCD(x, y), y)$ è iniettiva, surgettiva, bigettiva.

Esercizio 10.28. Risolvere l'equazione diofantea

$$40x + 252y = 44$$

Esercizio 10.29. Trovare tutte le soluzioni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ della equazione diofantea

$$4060x + 1953y = 49$$

È vero che per ogni soluzione $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ vale che $x - y$ è un multiplo di 3?

Esercizio 10.30. Calcolare il MCD $(1573, 1144)$ e trovare tutti gli interi m, n che soddisfano

$$1573m + 1144n = 858$$

Esercizio 10.31. Si determini l'insieme $A = \{(x, y) \in \mathbb{Z}^2 \mid 102x + 153y = 459\}$ Si determini la cardinalità dell'insieme $B = \{(x, y) \in A \mid |x| + |y| < 100\}$.

CAPITOLO 11

Numeri primi e congruenze

1. Alcune riflessioni sui numeri primi

Nelle lezioni precedenti abbiamo più volte chiamato in gioco i numeri primi. Dedichiamo loro un breve paragrafo in cui si accosta alla definizione tradizionale una definizione alternativa, e si cominciano a mettere a fuoco i due concetti di *elemento primo* e di *elemento irriducibile* di un anello. Dimostreremo anche il teorema della fattorizzazione unica, utilizzando il Teorema 10.15.

Cominciamo ricordando la più nota definizione di numero primo:

DEFINIZIONE 11.1. Un numero intero $p \geq 2$ si dice primo se gli unici suoi divisori interi positivi sono 1 e p stesso.

Ecco i numeri primi più piccoli: 2,3,5,7,11,13,17,19,23,29,31.

Anche se non abbiamo ancora introdotto la definizione formale di anello (che avete però visto al corso di Geometria 1), osserviamo che in questa prima definizione si mette in evidenza il fatto che i numeri primi sono elementi *irriducibili* di $\mathbb{Z}$, ossia elementi che non hanno una fattorizzazione 'vera': ogni volta che si scrive un numero primo p come prodotto $p = st$, visto che gli unici divisori di p sono 1 e p stesso, uno fra i numeri s o t è uguale a 1 o a -1, dunque è un elemento invertibile di $\mathbb{Z}$. In altre parole, ogni volta che si prova a fattorizzare p come prodotto di due fattori, uno dei due fattori è per forza invertibile.

Cerchiamo ora un'altra caratterizzazione dei numeri primi.

TEOREMA 11.2. *Sia p un numero primo. Supponiamo che, dati due numeri interi b, c, valga $p \mid bc$: allora possiamo concludere che o $p|b$ o $p|c$.*

DIMOSTRAZIONE. Se $p|b$ abbiamo finito. Consideriamo allora il caso in cui p non divide b; allora vale che $MCD(p, b) = 1$.[1]

Possiamo dunque applicare il Teorema 10.15: visto che $p \mid bc$ e che $MCD(p, b) = 1$ tale teorema ci dice che $p|c$. Dunque abbiamo dimostrato che o $p|b$ o $p|c$.

□

Vale anche il viceversa del Teorema 11.2:

TEOREMA 11.3. *Sia a un numero intero ≥ 2 con la seguente proprietà: per ogni $b, c \in \mathbb{Z}$, se $a \mid bc$ allora o $a|b$ o $a|c$. Allora a è un numero primo.*

DIMOSTRAZIONE. Dimostriamo la contronominale, ossia che se a non è primo, allora a non soddisfa la proprietà. Infatti se a non è primo allora deve avere un divisore positivo k diverso da 1 e da a, dunque deve valere

$$a = ks \qquad \text{con} \quad 1 < k < a \quad \text{e} \quad 1 < s < a$$

[1]Infatti $MCD(p, b)$ deve essere in particolare un divisore positivo di p, dunque ci sono solo due possibilità: $MCD(p, b) = 1$ o $MCD(p, b) = p$. La seconda però nel nostro caso è esclusa perché allora varrebbe $p|b$.

Ponendo $k = b$ e $s = c$ abbiamo allora trovato due numeri interi tali che $a \mid bc$ ma a non divide né b né c, ossia abbiamo mostrato che a non soddisfa la proprietà.

□

Gli enunciati dei due teoremi precedenti ci danno la seguente caratterizzazione dei numeri primi:

Teorema 11.4. *Un numero intero $p \geq 2$ è primo se e solo se soddisfa la seguente proprietà: per ogni $b, c \in \mathbb{Z}$, se $p \mid bc$ allora o $p|b$ o $p|c$.*

Osservazione 11.5. L'enunciato di questo teorema costituisce una definizione alternativa di numero primo. Questa nuova definizione mette in evidenza il fatto che un numero primo è un *elemento primo* dell'anello $\mathbb{Z}$. In un anello, un elemento γ si dice *primo* se, comunque si prendano α, β elementi dell'anello tali che $\gamma|\alpha\beta$ allora si ha che $\gamma|\alpha$ o $\gamma|\beta$. Anche se abbiamo appena visto che in $\mathbb{Z}$ i concetti di elemento irriducibile e di elemento primo coincidono, in generale per altri anelli non è così: in certi anelli l'insieme degli elementi irriducibili e l'insieme degli elementi primi non coincidono. Approfondiremo questo aspetto più avanti.

Possiamo a questo punto discutere la proprietà, ben nota fin dalle scuole medie, che ogni numero intero ammette una fattorizzazione unica come prodotto di primi.

Spezziamo il discorso in due parti: innanzitutto mostriamo che ogni numero si fattorizza in prodotto di primi.

Teorema 11.6 (Esistenza della fattorizzazione in prodotto di primi). *Ogni numero intero ≥ 2 o è primo o si può scrivere come prodotto di numeri primi.*

Dimostrazione. Questa dimostrazione è un facile esercizio di induzione. Utilizzeremo qui il principio del minimo.

Consideriamo il predicato $P(n)$: "il numero n o è primo o si può scrivere come prodotto di numeri primi" e sia S l'insieme dei numeri interi $m \geq 2$ tali che la proposizione $P(m)$ sia falsa.

Osserviamo che dimostrare l'enunciato del teorema equivale a dimostrare che S è vuoto. Procediamo per assurdo e supponiamo dunque che S non sia vuoto. Allora S, che è un sottoinsieme non vuoto di $\mathbb{N}$, per il principio del minimo ha un elemento minimo, che chiamiamo s.

Riassumendo, cosa sappiamo di s ? Sappiamo che è un intero ≥ 2 tale che $P(s)$ è falsa, ossia che non è né primo né prodotto di primi, e che è il più piccolo numero con queste caratteristiche.

In particolare, non essendo primo si potrà scrivere come prodotto di due numeri a e b, $s = ab$, dove $1 < a < s$ e $1 < b < s$. Quindi a e b, essendo ≥ 2 e strettamente minori di s, sono tali che le proposizioni $P(a)$ e $P(b)$ sono vere (altrimenti sarebbe uno di loro, e non s, il minimo dell'insieme S). Questo vuol dire che a e b sono o primi o prodotto di primi e dunque il prodotto ab ci fornisce una decomposizione in primi di s. Abbiamo ottenuto un assurdo, perché s per costruzione non può ammettere una decomposizione in primi.

□

Esercizio 11.7. Riscrivere la dimostrazione appena vista utilizzando l'induzione 'forte' o l'induzione 'semplice'.

Teorema 11.8 (Unicità della fattorizzazione in prodotto di primi). *Siano*

$$a = p_1 p_2 p_3 \cdots p_r$$

$$a = q_1 q_2 \cdots q_s$$

due fattorizzazioni del numero intero $a \geq 2$, dove i numeri p_i $(i = 1, 2, \ldots, r)$ e q_j $(j = 1, 2, \ldots, s)$ sono primi. Supponiamo di avere scritto le fattorizzazioni in modo che $p_1 \leq p_2 \leq \cdots \leq p_r$ e $q_1 \leq q_2 \leq \cdots \leq q_s$. Allora vale che $r = s$ e, per ogni $i = 1, 2, \ldots, s$, $p_i = q_i$.

Dimostrazione. Sia $r \leq s$ e dimostriamo il teorema per induzione su r. Il passo base $r = 1$ è semplice: s deve essere uguale ad 1 altrimenti il numero a sarebbe contemporaneamente primo ($a = p_1$) e non primo ($a = q_1 \cdots q_s$). A quel punto è immediato concludere che $a = p_1 = q_1$.

Per il passo induttivo, supponiamo che l'enunciato del teorema sia vero quando la prima fattorizzazione ha $r - 1$ fattori primi.

Cominciamo considerando il primo p_1. Visto che p_1 divide $q_1 q_2 \cdots q_s = q_1(q_2 \cdots q_s)$, per il Teorema 11.2 o $p_1 | q_1$ oppure $p_1 | (q_2 \cdots q_s)$. Se vale $p_1 | q_1$ allora, visto che p_1 e q_1 sono entrambi primi, deve valere $p_1 = q_1$. Dimostriamo per assurdo che deve essere proprio così. Se invece non valesse $p_1 | q_1$ allora avremmo $p_1 | (q_2 \cdots q_s)$ da cui, iterando il ragionamento, potremmo alla fine trovare dopo un numero finito di passi un i tale che $p_1 = q_i > q_1$ (se fosse $q_i = q_1$ allora fin dall'inizio avremmo trovato $p_1 | q_1$). Dunque q_1, essendo strettamente minore di p_1, è strettamente minore di tutti i primi p_i.

Ma noi sappiamo che q_1 divide $p_1(p_2 \cdots p_r)$. Con ragionamento analogo al precedente potremmo trovare un j tale che $q_1 = p_j$, ma questo è assurdo, visto che q_1 è strettamente minore di tutti i primi p_i.

Dunque deve valere $p_1 = q_1$. Dividendo l'uguaglianza $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ per p_1 otteniamo $p_2 \cdots p_r = q_2 \cdots q_s$, dove a sinistra abbiamo il prodotto di $r - 1$ fattori e a destra abbiamo $s - 1$ fattori.

Per ipotesi induttiva sappiamo che $r - 1 = s - 1$ e che i primi presenti nelle due fattorizzazioni sono a due a due uguali. Questo conclude la dimostrazione.

□

Esercizio 11.9. Alla luce del teorema di esistenza e unicità della fattorizzazione in primi riprendiamo in considerazione il metodo per la ricerca del massimo comune divisore fra due numeri a e b che si basa sulla scomposizione di a e b in fattori primi (descritto nel Capitolo 10, Paragrafo 2). Come mai questo metodo dà effettivamente il $MCD(a, b)$?

Concludiamo queste riflessioni sui numeri primi con il famoso teorema che ci garantisce che i numeri primi sono infiniti.

Teorema 11.10. *L'insieme $\mathcal{P}$ dei numeri primi è infinito.*

Dimostrazione. Supponiamo per assurdo che $\mathcal{P}$ sia finito e siano dunque

$$p_1, p_2, \ldots, p_N$$

tutti i numeri primi. Consideriamo allora il numero

$$a = (p_1 \cdot p_2 \cdots p_N) + 1$$

Per il Teorema 11.6 c'è un numero primo che divide a. Nel nostro caso vuol dire che uno dei p_i deve dividere a. Ma nessuno dei numeri p_i divide a, visto che, per ogni $i = 1, 2, \ldots, N$, da $a = (p_1 \cdot p_2 \cdots p_N) + 1$ si deduce che il resto della divisione euclidea di a per p_i è 1.

□

Curiosità: avete letto il libro del celebre matematico G.H. Hardy *Apologia di un matematico*? Ve lo consiglio. La dimostrazione che abbiamo appena visto compare come esempio di dimostrazione matematicamente "bella" e significativa.

2. Congruenze

Fissiamo un numero m intero positivo, per esempio $m = 12$.

Fare l'aritmetica modulo 12 vuol dire considerare tutti gli altri numeri interi da un punto di vista particolare: di ogni numero n ci interesserà solo il suo resto quando facciamo la divisione euclidea per 12. Per esempio, 38 sarà identificato al numero 2, visto che:

$$38 = 12 \cdot 3 + 2$$

Ma anche 62 sarà identificato al 2:

$$62 = 12 \cdot 5 + 2$$

Altri esempi, dove la freccia indica il resto della divisione per 12:

$$43 \to 7 \qquad 12 \to 0 \qquad -6 \to 6 \qquad -11 \to 1$$

$$15 \to 3 \qquad 27 \to 3 \qquad -8 \to 4 \qquad -12 \to 0$$

Si dirà per esempio che 38, 62 e 2 sono "congrui fra loro" modulo 12, e si scriverà:

$$38 \equiv 62 \equiv 2 \quad (12)$$

Pensandoci bene, questa è una aritmetica molto naturale per le lancette del nostro orologio: se si parte dalla mezzanotte di un certo giorno e si lasciano trascorrere due ore, le lancette indicheranno le 2. Ma anche se facciamo trascorrere 38 ore o 62 ore, le lancette indicheranno sempre le 2. Per le lancette del nostro orologio, i numeri 2, 68 e 38 sono in effetti "identificati"!

Dall'esempio passiamo ad una definizione più generale:

Definizione 11.11. Fissato un numero intero positivo m, diremo che due numeri interi a e b sono "congrui fra loro modulo m" se quando facciamo la divisione euclidea di a per m otteniamo lo stesso resto di quando facciamo la divisione euclidea di b per m. Scriveremo:

$$a \equiv b \qquad (m)$$

oppure

$$a \equiv b \qquad mod\ m$$

Se due numeri a e b sono congrui fra loro modulo m, possiamo scrivere le loro divisioni euclidee per m, che, come sappiamo, hanno lo stesso resto:

$$a = mq + r \qquad b = ms + r$$

Notiamo allora che

$$a - b = mq + r - (ms + r) = mq - ms = m(q - s)$$

Questo significa che m divide $a - b$. Viceversa, se prendiamo due numeri a e b che non sono congrui fra loro modulo m, possiamo facilmente osservare che $a-b$ non è un multiplo di m. Infatti, poniamo $a = mq + r_1$ e $b = ms + r_2$, dove r_1 e r_2 sono diversi fra loro e possiamo supporre $r_1 > r_2$. Scrivendo

$$a - b = mq + r_1 - (ms + r_2) = m(q - s) + (r_1 - r_2)$$

si nota che la divisione euclidea di $a - b$ per m ha resto $r_1 - r_2$, che è diverso da 0. In conclusione, abbiamo dimostrato:

PROPOSIZIONE 11.12. *Dato un numero intero positivo m, due numeri interi a e b sono congrui fra loro modulo m se e solo se m divide $a-b$ (questo equivale anche a dire che m divide $b-a$).*

OSSERVAZIONE 11.13. Dunque, la condizione "m divide $a-b$" poteva essere presa come definizione di congruenza fra i numeri interi a e b.

TEOREMA 11.14. *Le congruenze "rispettano" somme e prodotti, nel senso che se $a \equiv a' \bmod m$ e $b \equiv b' \bmod m$, allora $a+b \equiv a'+b' \bmod m$ e $ab \equiv a'b' \bmod m$.*

DIMOSTRAZIONE. Supponiamo che $a' = a + km$ e $b' = b + k'm$.
Allora $a' + b' = a + b + (k + k')m$, e quindi $a + b \equiv a' + b' \bmod m$.
Inoltre $a'b' = (a+km)(b+k'm) = ab+kmb+k'ma+kk'm^2$, e siccome $kmb+k'ma+kk'm^2$ è un multiplo di m possiamo concludere $a'b' \equiv ab \bmod m$. □

ESEMPIO 11.15. Trovare il resto della divisione euclidea di $1253423 \cdot 134432$ per 5. Visto che $1253423 \equiv 3 \bmod 5$ e che $134432 \equiv 2 \bmod 5$, possiamo sostituire e scrivere: $1253423 \cdot 134432 \equiv 3 \cdot 2 \equiv 6 \equiv 1 \bmod (5)$. Quindi il resto è 1.

ESEMPIO 11.16. Trovare il resto della divisione euclidea di 2^{99} per 7. Soluzione: $2^{99} = 2^{3 \cdot 33} = 8^{33}$. Ora, 8 è congruo a 1 modulo 7 dunque possiamo continuare sostituendo: $8^{33} \equiv 1^{33} \equiv 1 \bmod 7$. Quindi il resto è 1.

ESEMPIO 11.17. Trovare il resto della divisione di 3^{11} per 5. Soluzione: Modulo 5 abbiamo le seguenti congruenze: $3^{11} \equiv 3^2 3^2 3^2 3^2 3^2 3 \equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 3 \equiv (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot 3 \equiv -3 \equiv 2 \bmod (5)$. Quindi il resto è 2.

3. Calcolo veloce dei resti e basi numeriche

Ricordiamo che quando scriviamo un numero, ad esempio 1234567, implicitamente sottintendiamo che esso è scritto in base 10, ovvero:

$$1234567 = 1 \cdot 10^6 + 2 \cdot 10^5 + 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 + 7$$

Utilizzando il linguaggio delle congruenze possiamo trovare dei modi rapidi di calcolare il resto della divisione euclidea. I prossimi esempi illustrano il caso in cui il divisore è $3, 9, 11, 4, 7$ (e in particolare ci fanno riottenere i famosi criteri di divisibilità per $3, 4, 7, 11$).

ESEMPIO 11.18. Trovare il resto della divisione di 1234564 per 3. Soluzione: Siccome $10 \equiv 1 \bmod 3$, nel fare le congruenze modulo 3 possiamo sostituire 10 con 1 nell'espansione decimale ottenendo: $1234564 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 4 \equiv 1 \bmod 3$. Quindi il resto è 1. Se avessimo cercato il resto della divisione di 1234564 per 9, avremmo anche in questo caso sostituito il 10 con 1 ottenendo $1234564 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 4 \equiv 7 \bmod 9$.

ESEMPIO 11.19. Trovare il resto della divisione di 1234567 per 11. Soluzione: Siccome $10 \equiv -1 \bmod (11)$, nel fare le congruenze modulo 11 possiamo sostituire 10 con -1 nell'espansione decimale ottenendo: $1234567 \equiv 1 - 2 + 3 - 4 + 5 - 6 + 7 \equiv 4$. Quindi il resto è 4.

ESEMPIO 11.20. Trovare il resto della divisione di 1234567 per 4. Soluzione: osserviamo che $100 = 25 \cdot 4 \equiv 0 \bmod (4)$. Quindi $1234567 = 12345 \cdot 100 + 67 \equiv 67 \equiv 3 \bmod (4)$.

ESEMPIO 11.21. Trovare il resto della divisione di 1234567 per 7. Soluzione: osserviamo che $1000 = 7 \cdot 143 - 1 \equiv -1 \bmod (7)$. Quindi $1234567 = 1 \cdot 1000^2 + 234 \cdot 1000 + 567 \equiv 1 - 234 + 567 \equiv 334 \equiv 5 \bmod 7$.

Esempio 11.22. Si dimostri che $\sqrt{1234567}$ non è un intero. Soluzione: per assurdo supponiamo che vi sia un intero x tale che $x^2 = 1234567$. Per l'esercizio precedente $x^2 \equiv 1234567 \equiv 3 \bmod 4$. Quindi basta mostrare che x^2 non può essere congruente a 3 modulo 4. Siccome x è congruo a $0, 1, 2$ o 3 modulo 4, ci sono solo quattro verifiche da fare:

$$\begin{aligned} 0^2 &\equiv 0 \bmod 4 \\ 1^2 &\equiv 1 \bmod 4 \\ 2^2 &\equiv 0 \bmod 4 \\ 3^2 &\equiv 1 \bmod 4 \end{aligned}$$

Esempio 11.23. Cambiamento di base: verifichiamo che la scrittura (12345) in base 10 e la scrittura 30071 in base 8 indicano lo stesso numero. In simboli $(12345)_{\text{base } 10} = (30071)_{\text{base } 8}$. Infatti

$$\begin{aligned} 12345 &= 8 \cdot 1543 + 1 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= 8 \cdot 3 + 0 \\ 3 &= 8 \cdot 0 + 3 \end{aligned}$$

I resti danno la scrittura in base 8 richiesta: infatti da quanto abbiamo scritto segue che $12345 = 1543 \cdot 8 + 1 = 192 \cdot 8^2 + 7 \cdot 8 + 1 = 24 \cdot 8^3 + 7 \cdot 8 + 1 = 3 \cdot 8^4 + 7 \cdot 8 + 1$.

4. Inverso di un numero modulo un intero positivo

Gli unici numeri interi che ammettono un inverso moltiplicativo in $\mathbb{Z}$ sono $+1$ e -1. Quando si considera l'aritmetica modulo un intero positivo m, invece sarà naturale trovare vari numeri che ammettono un inverso. Naturalmente, in questo caso per dire che un numero è inverso di un altro non pretendiamo che il prodotto dei due numeri faccia 1, ma ci basta che faccia un qualunque numero *congruo* a 1:

Definizione 11.24. Sia m un intero positivo. Un inverso di un intero a modulo m è un intero x tale che $ax \equiv 1 \bmod m$.

Esempio 11.25. 2 è un inverso di 3 modulo 5 in quanto $2 \cdot 3 = 6 \equiv 1 \bmod 5$. Attenzione, anche 7 è un inverso di 3, e anche -3...Come potete facilmente verificare, quando un numero ammette un inverso modulo m non ne ammette uno solo, ma infiniti.

Esempio 11.26. Non ci sono inversi di 2 modulo 4.

Teorema 11.27. *Un numero a ha un inverso modulo m se e solo se $MCD(a, m) = 1$.*

Dimostrazione. Se $MCD(a, m) = 1$ per il teorema di Bezout possiamo trovare u, v interi tali che $au + mv = 1$ con u, v interi. Questa uguaglianza, letta modulo m, diventa $au \equiv 1 \bmod m$. Quindi u è un inverso di a modulo m.

Viceversa supponiamo che a abbia un inverso u modulo m, ovvero $au \equiv 1 \bmod m$; allora per definizione di congruenza esiste k tale che $au + mk = 1$. Questo implica (per il Teorema 10.13) $MCD(a, m) = 1$. □

Non sempre possiamo dividere in una congruenza. Ad esempio $2 \cdot 7 \equiv 2 \cdot 4 \bmod 6$, ma $7 \not\equiv 4 \bmod 6$. In generale, la divisione in una congruenza segue la seguente regola:

Teorema 11.28. *Dato $m \in \mathbb{N} - \{0\}$, per ogni $a \in \mathbb{Z} - \{0\}$, $b_1, b_2 \in \mathbb{Z}$ vale:*

$$a\ b_1 \equiv a\ b_2 \quad (m) \quad \Leftrightarrow \quad b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a, m)}\right)$$

Osservazione 11.29. Quindi, se c'è un numero a che divide entrambi i membri di una congruenza, si può "semplificare", a patto però di dividere anche il modulo m per $MCD(a, m)$. Ad esempio:

$$66 \equiv 42 \quad (8) \quad \Leftrightarrow \quad 11 \equiv 7 \quad (4)$$

dove abbiamo diviso il membro di sinistra e quello di destra per 6 e il modulo per $MCD(6, 8) = 2$. Se non avessimo diviso il modulo per 2 avremmo ottenuto

$$11 \equiv 7 \quad (8)$$

che è **falsa**.

Dimostrazione. Ricordiamo che stiamo considerando $a \in \mathbb{Z} - \{0\}$. Supponiamo che

$$a\ b_1 \equiv a\ b_2 \quad (m)$$

Allora per la definizione di congruenza vale che

$$m \mid ab_1 - ab_2$$

ossia esiste un $q \in \mathbb{Z}$ tale che

$$ab_1 - ab_2 = mq$$

Possiamo dividere per $MCD(a, m)$ e otteniamo

$$\frac{a}{MCD(a,m)}(b_1 - b_2) = \frac{m}{MCD(a,m)}q$$

Da questo, visto che $\frac{a}{MCD(a,m)}$ e $\frac{m}{MCD(a,m)}$ sono coprimi (ricordate il Corollario 10.14), segue, per il Teorema 10.15, che

$$\frac{m}{MCD(a,m)} \mid b_1 - b_2$$

ovvero che

$$b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a,m)}\right)$$

Supponiamo ora, viceversa, che sia vero

$$b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a,m)}\right)$$

Allora $\frac{m}{MCD(a,m)} \mid (b_1 - b_2)$, ossia esiste un $t \in \mathbb{Z}$ tale che

$$t\frac{m}{MCD(a,m)} = b_1 - b_2$$

da cui, moltiplicando per $MCD(a, m)$ otteniamo

$$tm = (b_1 - b_2)MCD(a, m)$$

Osserviamo dunque che

$$m \mid (b_1 - b_2)MCD(a, m)$$

da cui a maggior ragione ricaviamo

$$m \mid (b_1 - b_2)a$$

(abbiamo usato il fatto che $MCD(a, m)|a$) che si riscrive come

$$a\ b_1 \equiv a\ b_2 \quad (m)$$

□

COROLLARIO 11.30. *Se* $ac \equiv bc \quad (m)$ *e* $MCD(c, m) = 1$, *allora* $a \equiv b \quad (m)$.

5. Esercizi

ESERCIZIO 11.31. Sia $\{a_n\}_{n\in\mathbb{N}}$ la successione definita per ricorrenza da

$$\begin{aligned} a_0 &= 2 \\ a_1 &= 1 \\ a_{n+1} &= 2a_n + 3a_{n-1} \qquad \forall n \geq 1. \end{aligned}$$

Dimostrare che:

(1) MCD$(a_n, 3) = 1$ per ogni $n \geq 0$.
(2) MCD$(a_{n+1}, a_n) = 1$ per ogni $n \geq 0$.

ESERCIZIO 11.32. Dimostrare che l'insieme dei numeri primi congrui a 3 modulo 4 è infinito.[2]

ESERCIZIO 11.33. Consideriamo i numeri interi x tali che $10000000 \leq x < 20000000$. Quanti di questi numeri sono congrui a 1 modulo 3?

ESERCIZIO 11.34. Stabilire se è vero o falso che

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot 12 \cdot 13 \equiv 7 \qquad (17)$$

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot 12 \cdot 13 \equiv 0 \qquad (1024)$$

In generale è vero o falso che il prodotto di 13 numeri interi consecutivi è sempre divisibile per 1024 ?

ESERCIZIO 11.35. Consideriamo la successione definita per ricorrenza

$$x_0 = 2, \; x_{n+1} = (x_n^2 + 1)$$

Sia r_n il resto della divisione euclidea di x_n per 5.

1) Calcolare i primi 7 valori di r_n.

2) Si dia una regola generale per calcolare r_n e la si dimostri per induzione.

3) Si calcoli r_{10000}.

ESERCIZIO 11.36 (Tornei all'italiana). Supponiamo di avere n squadre di calcio, con n numero pari, e di voler organizzare un torneo all'italiana[3]. Basta pensare al girone d'andata, quello di ritorno poi è automatico, dunque bisogna organizzare $n-1$ turni. Le congruenze possono aiutarci. Possiamo infatti utilizzare la seguente regola:

[2]Anche l'insieme dei numeri primi congrui a 1 modulo 4 è infinito, ma di questo parleremo più avanti.

[3]Se avessimo un numero dispari di squadre ci potremmo comunque ricondurre a questo caso aggiungendo una squadra fittizia, con la regola che se una squadra deve incontrarla le tocca invece un turno di riposo.

- al turno i la squadra x, con $1 \leq x \leq n-1$, incontrerà la squadra y dove y soddisfa $1 \leq y \leq n-1$ e

$$x + y \equiv i \mod n - 1$$

a meno che questa equazione non dia come soluzione $x = y$. In tal caso la squadra x incontra la squadra n.

Dimostrare che il torneo così preparato è ben organizzato (vedi Tabella 1).

	Turno 1	Turno 2	Turno 3	Turno 4	Turno 5
squadra 1	vs 5	vs 6	vs 2	vs 3	vs 4
squadra 2	vs 4	vs 5	vs 1	vs 6	vs 3
squadra 3	vs 6	vs 4	vs 5	vs 1	vs 2
squadra 4	vs 2	vs 3	vs 6	vs 5	vs 1
squadra 5	vs 1	vs 2	vs 3	vs 4	vs 6
squadra 6	vs 3	vs 1	vs 4	vs 2	vs 5

TABELLA 1. Esempio: il tabellone del torneo nel caso di 6 squadre.

ESERCIZIO 11.37. Dato un numero naturale m, dimostrare che se $2^m + 1$ è primo allora m è una potenza di 2.

ESERCIZIO 11.38 (I numeri di Fermat). Dato $n \in \mathbb{N}$ definiamo:

$$\mathcal{F}_n = 2^{2^n} + 1$$

I numeri $\mathcal{F}_n$ si chiamano *numeri di Fermat*. Fermat[4] aveva congetturato che tali numeri fossero tutti primi..ma, come fu mostrato da Eulero[5], la congettura è falsa. Provate anche voi a confutarla:

- Dimostrare che $\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ sono primi. Dimostrare che anche $\mathcal{F}_4$ è primo. [Consiglio: non fatelo davvero, $\mathcal{F}_4$ è un numero troppo grande. La cosa diventerà abbordabile dopo che saprete i risultati degli Esercizi 14.39 e 14.40.]
- Dimostrare che $\mathcal{F}_5$ è divisibile per 641. [Traccia: può essere utile osservare che $641 = 2^4 + 5^4 = 1 + 5 \cdot 2^7$]

[4]Pierre de Fermat, matematico francese, 1601-1665.

[5]Leonhard Euler, matematico svizzero, 1707-1783.

Possiamo comunque utilizzare i numeri di Fermat per dimostrare, in maniera diversa da quella del Teorema 11.10, che i numeri primi sono infiniti:

- Dimostrare che se $n \neq m$ allora $\mathcal{F}_n$ e $\mathcal{F}_m$ sono coprimi.
- Dedurre dal punto precedente che i numeri primi sono infiniti.

CAPITOLO 12

Congruenze lineari

1. Metodo per risolvere le congruenze lineari in una incognita

In questo paragrafo ci occuperemo della risoluzione di congruenze lineari con una incognita, ossia del seguente problema:

dati $a, b, m \in \mathbb{Z}$ con $m > 0$, trovare tutti i numeri interi che risolvono la congruenza lineare ad una incognita

$$ax \equiv b \bmod (m) \tag{1}$$

Innanzitutto osserviamo che se esiste un intero d che divide a e m ma non divide b, allora l'equazione (1) non ha soluzioni. Infatti se (1) ha una soluzione $\overline{x}$, allora esiste un intero k tali che $a\overline{x} - b = km$. Da questa uguaglianza si ricava subito che se d divide a e m allora deve dividere anche b.

Esempio 12.1. $6x \equiv 3 \bmod 4$ non ha soluzioni perché 2 divide 6 e 4 ma non divide 3.

In particolare dalla osservazione precedente si deduce che una condizione necessaria perchè l'equazione (1) abbia soluzioni è che $MCD(a, m)$ divida b. Sempre riflettendo sulla osservazione precedente, ci si accorge che in realtà il problema di risolvere $ax \equiv b \bmod (m)$ è in sostanza la stessa cosa del problema di risolvere l'equazione diofantea $ax - km = b$ nelle variabili x e k. Dunque potremmo già concludere che la condizione che $MCD(a, m)$ divida b è anche sufficiente per l'esistenza di soluzioni della equazione (1).

Enunceremo però tutto questo nel prossimo teorema, e daremo una dimostrazione che fornirà anche un algoritmo per trovare tutte le soluzioni quando esistono. Prima di enunciarlo, però, è bene fare una osservazione su quando due equazioni sono equivalenti.

Osservazione 12.2. Dato un numero k che divide a e b, l'equazione

$$\frac{a}{k}x \equiv \frac{b}{k} \quad \left(\frac{m}{MCD(k, m)}\right)$$

è equivalente alla equazione (1), ossia *ha le stesse soluzioni*. Questo segue dalla regola di divisione data dal Teorema 11.28, visto che in base a tale regola un intero $\overline{x}$ soddisfa $a\overline{x} \equiv b \quad (m)$ se e solo se soddisfa

$$\frac{a}{k}\overline{x} \equiv \frac{b}{k} \quad \left(\frac{m}{MCD(k, m)}\right)$$

Analogamente (si può vedere in realtà come caso particolare di quanto appena osservato), se s è un numero primo con m, l'equazione

$$sax \equiv sb \quad (m)$$

è equivalente alla (1).

Teorema 12.3. *La congruenza*

$$ax \equiv b \quad (m) \tag{1}$$

ha soluzione se e solo se il massimo comun divisore tra a e m divide b. In questo caso l'equazione ha infinite soluzioni, precisamente $MCD(a, m)$ soluzioni modulo m.

Osservazione 12.4. Quando diciamo "l'equazione ha $MCD(a, m)$ soluzioni modulo m" intendiamo dire che l'insieme delle soluzioni dell'equazione è composto da esattamente $MCD(a, m)$ soluzioni $\overline{x}$ che soddisfano $0 \leq \overline{x} < m$ e tutte le altre soluzioni sono i numeri che si ottengono da queste sommando loro un multiplo di m.

Dimostrazione. Se $MCD(a, m)$ non divide b sappiamo già che la congruenza non ha soluzioni. Quindi consideriamo il caso in cui $MCD(a, m)$ divide b. In questo caso $MCD(a, m)$ è dunque il massimo divisore positivo comune a tutti e tre i numeri a, b, m; dividendo l'equazione data per $MCD(a, m)$ otteniamo l'equazione

$$a'x \equiv b' \quad (m') \tag{$*$}$$

dove $a' = \dfrac{a}{MCD(a,m)}, b' = \dfrac{b}{MCD(a,m)}, m' = \dfrac{m}{MCD(a,m)}$, che è equivalente alla (1) come sappiamo dalla Osservazione 12.2.

A questo punto notiamo che, per costruzione, a' e m' sono coprimi e che, per il Teorema 11.28, a' ha un inverso e' modulo m'. [1] Osserviamo in particolare che, visto che anche e' ha un inverso modulo m', ovvero a', allora per il Teorema 11.28 risulta che e' è primo con m'.

Moltiplicando per e' il membro di sinistra e quello di destra di $(*)$ otteniamo

$$e'a'x \equiv e'b' \quad (m') \tag{$**$}$$

Per l'Osservazione 12.2 sappiamo che l'equazione $(**)$ è equivalente alla $(*)$.

Visto che $e'a' \equiv 1 \quad (m')$ possiamo riscrivere la $(**)$ come

$$x \equiv e'b' \quad (m')$$

A questo punto si osserva subito che le soluzioni di questa equazione (e dunque le soluzioni della (1)) sono tutti e soli gli interi della forma $e'b' + km'$ al variare di k in $\mathbb{Z}$. Visto che $m' = \dfrac{m}{MCD(a,m)}$, ci sono esattamente $MCD(a, m)$ interi di questa forma in ogni sequenza di m numeri consecutivi. □

Esempio 12.5. Data l'equazione

$$195x \equiv 6 \quad (42)$$

trovare:
a) tutte le sue soluzioni,
b) le sue soluzioni modulo 42, ossia quelle comprese fra 0 e 41.

Soluzione: Osserviamo che $MCD(195, 42) = 3 \mid 6$ dunque l'equazione ha soluzione. Per prima cosa possiamo sostituire 195 con il suo resto modulo 42, ossia 27:

$$27x \equiv 6 \quad (42)$$

[1] Ricordiamo che, in concreto, si può applicare l'algoritmo per trovare una combinazione di Bezout per ottenere due interi x', y' tali che $1 = a'x' + m'y'$ e poi si prende $e' = x'$.

Poi possiamo dividere membro di destra, membro di sinistra e modulo per $MCD(195, 42) = 3$, ottenendo l'equazione equivalente:

$$9x \equiv 2 \quad (\frac{42}{MCD(3, 42)} = 14)$$

Un possibile modo di procedere adesso è il seguente: si nota "a occhio" che $3 \cdot 9 = 27$ è congruo a -1 modulo 14. Dunque ci conviene moltiplicare il membro di sinistra e quello di destra per 3. Visto che 3 è primo con 14, per l'Osservazione 12.2 sappiamo che l'equazione che otteniamo è equivalente:

$$27x \equiv 6 \quad (14)$$

che si può riscrivere

$$-x \equiv 6 \quad (14)$$

Moltiplicando adesso per -1 (anch'esso primo con 14), otteniamo:

$$x \equiv -6 \quad (14)$$

Questa scrittura descrive già con chiarezza l'insieme di tutte soluzioni dell'equazione

$$195x \equiv 6 \quad (42)$$

Possiamo comunque anche scriverlo così:

$$\{x = -6 + 14q \mid q \in \mathbb{Z}\}$$

Per rispondere alla domanda b), dobbiamo indicare le soluzioni x con $0 \leq x \leq 41$. Sono tre: $-6 + 14, -6 + 2 \cdot 14, -6 + 3 \cdot 14$, cioè 8, 22 e 36. □

2. Esempi di risoluzione di una equazione diofantea (usando le congruenze)

Facciamo qualche esempio che illustra la relazione fra le soluzioni di una equazione diofantea e quella delle equazioni lineari con congruenze ad essa associate. Consideriamo l'equazione diofantea:

$$224x + 108y = 700 \qquad (*)$$

Osservazione 12.6. Se esiste una soluzione (X, Y), il numero intero X deve anche soddisfare

$$224X \equiv 700 \quad (108)$$

(infatti $108Y = 700 - 224X$ dunque $108 \mid 224X - 700$). Viceversa, se un certo numero intero X soddisfa la congruenza $224X \equiv 700 \quad (108)$, questo vuol dire che soddisfa $108 \mid 224X - 700$; allora deve esistere un Y tale che $108Y = 700 - 224X$ e dunque

$$224X + 108Y = 700$$

cioè la coppia (X, Y) risolve l'equazione diofantea $(*)$.

In conclusione abbiamo osservato che l'insieme delle soluzioni dell'equazione

$$224x \equiv 700 \quad (108)$$

coincide con l'insieme dato dalle prime componenti ("le X") delle coppie che risolvono l'equazione diofantea $(*)$.

Risolviamo allora la congruenza

$$224x \equiv 700 \quad (108)$$

Osservazione 12.7. Per risolvere una equazione con congruenze o una equazione diofantea, come avete capito, ci sono molte strade diverse. In questi esempi noi presentiamo una possibile soluzione, ma voi potete divertirvi a trovarne altre, magari più rapide.

Per prima cosa osserviamo sostituiamo il 224 e il 700 con dei numeri più piccoli, a loro congrui modulo 108:

$$8x \equiv 160 \quad (108)$$

Ora possiamo dividere per 8, per semplificare[2] :

$$x \equiv 20 \quad (\frac{108}{MCD(108,8)} = 27)$$

Dunque l'insieme delle soluzioni di

$$224x \equiv 700 \quad (108)$$

è

$$\{x = 20 + 27q \mid q \in \mathbb{Z}\}$$

Possiamo sostituire queste soluzioni al posto della x nella equazione diofantea

$$224x + 108y = 700$$

(che comunque per semplificare possiamo dividere per 4=MCD (224, 108), ottenendo l'equazione diofantea equivalente $56x + 27y = 175$):

$$56(20 + 27q) + 27y = 175$$

Svolgiamo i conti:

$$27y = -1120 + 175 - 56 \cdot 27q$$
$$27y = -945 - 56 \cdot 27q$$
$$y = -35 - 56q$$

Abbiamo dunque trovato che l'insieme delle soluzioni di

$$224x + 108y = 700$$

è:

$$\{(20 + 27q \ , \ -35 - 56q) \mid q \in \mathbb{Z}\}$$

Esempio 12.8. Trovare tutte le soluzioni intere della equazione diofantea

$$54 = 252x + 198y.$$

Soluzione: Dividendo tutto per $18 = MCD(252, 198)$ otteniamo l'equazione equivalente:

$$3 = 14x + 11y$$

Risolviamo la congruenza

$$14x \equiv 3 \bmod 11$$

Moltiplicando per 4 e semplificando otteniamo $x \equiv 1 \bmod 11$, quindi x è della forma $x = 1 + 11k$. Sostituendo nella $14x + 11y = 3$ e facendo i conti si trova $y = -1 - 14k$. Dunque l'insieme delle soluzioni della equazione diofantea data è

$$\{(1 + 11k \ , \ -1 - 14k) \mid k \in \mathbb{Z}\}$$

□

Osserviamo che nei due esempi di questo paragrafo abbiamo trovato in un colpo solo tutte le soluzioni della diofantea, senza dividere il problema nella ricerca di una soluzione particolare e poi di tutte le soluzioni della omogenea associata. Di volta in volta potrete scegliere il metodo di risoluzione che vi sembra più conveniente.

[2]La scelta di sostituire il 700 con 160, anzichè per esempio col 52, è stata dettata proprio dal fatto di aver intravisto la possibilità di questa divisione per 8 che rende la soluzione molto rapida; la conclusione dell'esercizio sarebbe abbastanza veloce anche sostituendo con il 52, verificate.

3. Sistemi di congruenze. Il teorema cinese del resto

Proviamo a risolvere un sistema di due equazioni lineari con congruenze:

$$\begin{cases} x & \equiv & a & (m_1) \\ x & \equiv & b & (m_2) \end{cases}$$

Per prima cosa osserviamo che le soluzioni della prima equazione sono tutti e soli i numeri della forma

$$x = a + km_1 \quad \text{con} \quad k \in \mathbb{Z}$$

Ci chiediamo quando un tale numero risolve anche la seconda equazione. Per saperlo sostituiamo $a + km_1$ alla x nella seconda equazione:

$$a + km_1 \equiv b \qquad (m_2)$$

Qui la variabile è k e otteniamo

$$m_1 k \equiv b - a \qquad (m_2)$$

Questa equazione, come sappiamo, ha soluzione se e solo se $MCD(m_1, m_2) \mid (b - a)$. Dunque siamo già arrivati ad una prima conclusione: il sistema di partenza ha soluzione se e solo se $MCD(m_1, m_2) \mid (b - a)$.

Nel caso in cui ci siano soluzioni, come fare a trovarle tutte? Prendiamo una soluzione particolare k_0 della equazione

$$m_1 k \equiv b - a \qquad (m_2)$$

Allora $x_0 = a + k_0 m_1$ è una soluzione del sistema di partenza ossia

$$\begin{cases} x_0 & \equiv & a & (m_1) \\ x_0 & \equiv & b & (m_2) \end{cases}$$

Come differisce da un'altra soluzione del sistema di partenza? Se anche x_1 soddisfa

$$\begin{cases} x_1 & \equiv & a & (m_1) \\ x_1 & \equiv & b & (m_2) \end{cases}$$

sottraendo opportunamente otteniamo

$$\begin{cases} x_0 - x_1 & \equiv & 0 & (m_1) \\ x_0 - x_1 & \equiv & 0 & (m_2) \end{cases}$$

Dunque $x_0 - x_1$ è un numero che deve essere multiplo di m_1 e anche di m_2. Il più piccolo numero intero positivo che soddisfa tale condizione come sapete si chiama minimo comune multiplo di m_1 e di m_2 e si indica come $mcm\ (m_1, m_2)$. Ricordiamo anche che tutti e soli i numeri che sono divisi da m_1 e da m_2 sono i multipli di $mcm\ (m_1, m_2)$.[3]

In conclusione, tornando al nostro sistema, abbiamo dimostrato che due soluzioni x_0 e x_1 del sistema differiscono per un multiplo di $mcm\ (m_1, m_2)$. Viceversa si verifica subito che, dato x_0 che soddisfa il sistema e dato un multiplo $s \cdot mcm\ (m_1, m_2)$ di $mcm\ (m_1, m_2)$, anche

$$x_0 + s \cdot mcm\ (m_1, m_2)$$

soddisfa il sistema.

Possiamo riassumere tutto quel che abbiamo detto fin qui nel seguente:

[3] Infatti se t è diviso da m_1 e anche da m_2, consideriamo la divisione euclidea di t per $mcm\ (m_1, m_2)$:

$$t = q \cdot mcm\ (m_1, m_2) + r$$

dove $0 \leq r < mcm\ (m_1, m_2)$. Ora, siccome m_1 e m_2 dividono t e $q \cdot mcm\ (m_1, m_2)$, entrambi devono anche dividere r. Allora r deve essere 0, altrimenti sarebbe un numero intero positivo diviso da m_1 e da m_2 ma più piccolo di $mcm\ (m_1, m_2)$ (assurdo).

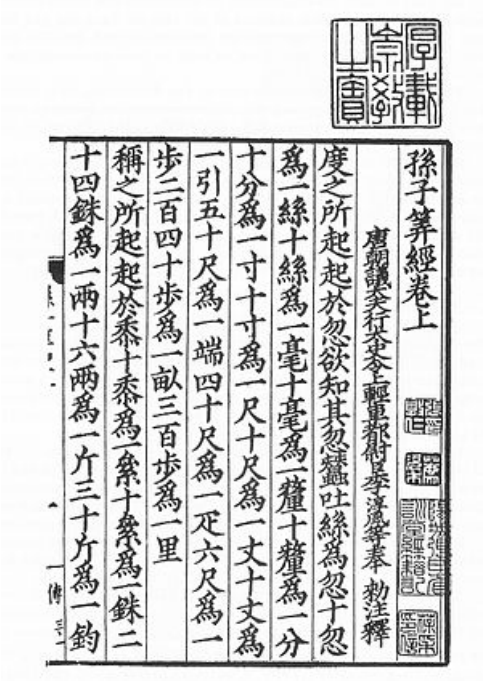

FIGURA 1. Una edizione del trattato Sunzi del V secolo, contenente una formulazione del Teorema Cinese del Resto (immagine da Wikipedia).

TEOREMA 12.9 (Teorema cinese del resto per due equazioni con moduli qualunque). *Dato il sistema di equazioni*

$$\begin{cases} x \equiv a & (m_1) \\ x \equiv b & (m_2) \end{cases}$$

tale sistema ammette soluzione se e solo se $MCD(m_1, m_2) \mid (b-a)$. *In tal caso, presa una soluzione* x_0*, tutte le altre soluzioni del sistema sono i numeri della forma*

$$x_0 + s \cdot mcm\ (m_1, m_2) \quad con \quad s \in \mathbb{Z}$$

OSSERVAZIONE 12.10. Come sappiamo, questo si può esprimere anche dicendo che tutte le soluzioni del sistema sono i numeri x che soddisfano

$$x \equiv x_0 \qquad (mcm\ (m_1, m_2))$$

In particolare osserviamo che esiste un'unica soluzione x con $0 \leq x < mcm\ (m_1, m_2)$.

ESEMPIO 12.11. Si consideri il sistema:

$$\begin{cases} 14x \equiv 4570 & (30) \\ 45x \equiv 231 & (8) \end{cases}$$

Innanzitutto studiamo e risolviamo una per una le due equazioni: la prima ha soluzione perché $MCD(14, 30) = 2 | 4570$ e la possiamo riscrivere sostituendo a 4570 il suo resto modulo 30:

$$14x \equiv 10 \qquad (30)$$

Dividendo per 2 otteniamo:

$$7x \equiv 5 \qquad (15)$$

Se moltiplichiamo entrambi i membri per 2 otteniamo una equazione equivalente perché 2 è primo con il modulo 15 e così arriviamo a

$$14x \equiv 10 \qquad (15)$$

$$-x \equiv 10 \qquad (15)$$

$$x \equiv -10 \qquad (15)$$

$$x \equiv 5 \qquad (15)$$

Per quel che riguarda la seconda equazione, notiamo subito che ha soluzione perché 45 e 8 sono primi fra loro. Sostituiamo ai numeri che compaiono i loro resti modulo 8:

$$5x \equiv 7 \qquad (8)$$

Moltiplicando entrambi i membri per 3 otteniamo l' equazione equivalente

$$15x \equiv 21 \qquad (8)$$

che risolviamo facilmente

$$-x \equiv 5 \qquad (8)$$

$$x \equiv -5 \qquad (8)$$

$$x \equiv 3 \qquad (8)$$

Dunque il sistema dato si può riscrivere come

$$\begin{cases} x \equiv 5 & (15) \\ x \equiv 3 & (8) \end{cases}$$

Ora possiamo applicare il teorema cinese del resto: il sistema ammette soluzione perché $MCD(15, 8) = 1$ e dunque divide $5 - 3$.

A questo punto dobbiamo trovare una soluzione particolare. Ne esisterà una (e una sola) compresa fra 0 e 119 (infatti $120 = 15 \cdot 8$ è il mcm $(15, 8)$). Possiamo cercarla fra i numeri $5, 20, 35, 50, 65, ...$ che sono le soluzioni della prima equazione. Vediamo subito che 35 fa al caso nostro. Dunque, grazie al teorema cinese del resto, possiamo affermare che tutte le soluzioni del sistema sono i numeri della forma

$$35 + 120s \qquad \text{con} \quad s \in \mathbb{Z}$$

Osservazione 12.12. Se non avessimo "visto" subito il 35 avremmo comunque potuto seguire il metodo standard: la prima equazione ci dice che x deve essere del tipo $x = 5 + 15k$. Sostituendo nella seconda abbiamo

$$5 + 15k \equiv 3 \qquad (8)$$

ossia

$$15k \equiv -2 \qquad (8)$$

$$-k \equiv -2 \qquad (8)$$

$$k \equiv 2 \qquad (8)$$

Allora $x = 5 + 15 \cdot 2 = 35$ è una soluzione particolare..e abbiamo "ritrovato" il 35.

Riscriviamo ora il teorema nel caso particolare in cui i moduli delle due equazioni sono primi fra loro, come premessa per poi enunciare il teorema cinese del resto nella sua forma classica.

TEOREMA 12.13 (Teorema cinese del resto per due equazioni con moduli primi fra loro). *Dato il sistema di congruenze*

$$\begin{cases} x & \equiv & a & (m_1) \\ x & \equiv & b & (m_2) \end{cases}$$

con $MCD(m_1, m_2) = 1$*, tale sistema ammette sempre soluzione ed esiste un'unica soluzione* x_0 *tale che* $0 \leq x_0 < m_1 \cdot m_2$*. Tutte le altre soluzioni del sistema sono i numeri della forma*

$$x_0 + q \cdot m_1 \cdot m_2 \quad con \quad q \in \mathbb{Z}$$

La dimostrazione che abbiamo dato si generalizza facilmente al caso di sistemi di n congruenze in cui i moduli siano a due a due coprimi:

TEOREMA 12.14 (Teorema cinese del resto, forma classica). *Dato il sistema di congruenze*

$$\begin{cases} x & \equiv & a_1 & (m_1) \\ x & \equiv & a_2 & (m_2) \\ .. & .. & .. & .. \\ .. & .. & .. & .. \\ x & \equiv & a_{n-1} & (m_{n-1}) \\ x & \equiv & a_n & (m_n) \end{cases}$$

in cui i moduli sono a due a due coprimi (questo vuol dire che per ogni $i \neq j$ *vale* $MCD(m_i, m_j) = 1$*), tale sistema ammette sempre soluzione ed esiste un'unica soluzione* x_0 *tale che* $0 \leq x_0 < m_1 \cdot m_2 \cdots m_{n-1} \cdot m_n$*. Tutte le altre soluzioni del sistema sono i numeri della forma*

$$x_0 + q \cdot m_1 \cdot m_2 \cdots m_{n-1} \cdot m_n \quad con \quad q \in \mathbb{Z}$$

ESERCIZIO 12.15. Dimostrare la forma classica del teorema cinese del resto. (Suggerimento: per induzione sul numero n di equazioni del sistema; il caso di sistemi con due congruenze lo abbiamo già studiato...).

Trovate una discussione del teorema cinese del resto nel libro [**?**], al Capitolo 4, Paragrafo 7 (in alcuni passaggi viene usata la notazione delle classi di resto, che noi introdurremo presto, ma alcuni esempi ed esercizi sono scritti nella stessa notazione che abbiamo usato noi).

4. Esercizi

ESERCIZIO 12.16. Risolvere l'equazione diofantea

$$40x + 252y = 44$$

Esistono soluzioni (x, y) con $x \equiv 0 \quad (7)$? E con $x \equiv 0 \quad (13)$?

SOLUZIONE: Innanzitutto notiamo che tutti i numeri che compaiono nella equazione sono divisibili per 4. Ci conviene dunque dividere per 4 e studiare l'equazione equivalente:

$$10x + 63y = 11$$

Questa ammette soluzione, visto che 10 e 63 sono primi fra loro e dunque $MCD(10, 63) \mid 11$.

A questo punto, per trovare le soluzioni, sono possibili varie strade. Ne mostriamo una, risolvendo l'equazione lineare con le congruenze:

$$63y \equiv 11 \quad (10)$$

Questa, visto che stiamo lavorando modulo 10, si può riscrivere come:

$$3y \equiv 1 \quad (10)$$

Si nota subito che ha la soluzione $y = -3$. Sappiamo poi, per il Teorema 12.3, che tutte le soluzioni sono gli interi della forma $y = -3 + 10k$ al variare di $k \in \mathbb{Z}$.

A fini puramente didattici, presentiamo in un altro modo l'ultimo passaggio, a partire da

$$3y \equiv 1 \quad (10)$$

Moltiplichiamo per 7 entrambi i membri della equazione (questo produce una equazione equivalente visto che 7 è primo con 10) e otteniamo:

$$21y \equiv 7 \quad (10)$$

ossia

$$y \equiv 7 \quad (10)$$

Da qui "leggiamo" di nuovo lo stesso insieme di soluzioni, presentato nella forma $y = 7 + 10k$ *al variare di* $k \in \mathbb{Z}$.

Sostituendo $y = -3 + 10k$ nella equazione diofantea

$$10x + 63y = 11$$

troveremo il corrispondente valore della x e, al variare di $k \in \mathbb{Z}$, tutte le coppie (x, y) che risolvono il problema posto nel testo:

$$10x + 63(-3 + 10k) = 11$$

$$10x = 200 - 630k$$

$$x = 20 - 63k$$

Dunque l'insieme di tutte le soluzioni della equazione diofantea data è:

$$\{(20 - 63k, -3 + 10k) \in \mathbb{Z} \times \mathbb{Z} \mid k \in \mathbb{Z}\}$$

Rispondiamo ora alle ultime due domande.

Possono esistere soluzioni (x, y) con $x \equiv 0 \quad (7)$? In altre parole, ci chiediamo se per certi valori di $k \in \mathbb{Z}$ può essere vera la congruenza

$$20 - 63k \equiv 0 \quad (7)$$

Ma, visto che stiamo lavorando modulo 7, e $-63k \equiv 0 \quad (7)$ questo equivale a chiedersi se è vera

$$20 \equiv 0 \quad (7)$$

e la risposta è NO.

Possono esistere soluzioni (x, y) con $x \equiv 0 \quad (13)$? Stavolta consideriamo

$$20 - 63k \equiv 0 \quad (13)$$

che si riscrive:

$$-63k \equiv -20 \quad (13)$$

$$63k \equiv 20 \quad (13)$$

$$11k \equiv 7 \quad (13)$$

Questa la si può considerare come una equazione con le congruenze con k come variabile; visto che $MCD(11, 13) = 1$ divide 7 sappiamo che tale equazione ha soluzione. Dunque possiamo rispondere che SÌ, possono esistere soluzioni (x, y) con $x \equiv 0 \quad (13)$.

Notiamo che l'esercizio non chiedeva di trovare le soluzioni, ma solo di dire se potevano esistere, motivando la risposta. Notiamo inoltre che a queste ultime due domande si

poteva rispondere anche prima di calcolare le soluzioni della equazione diofantea. La prima domanda, per esempio, equivale infatti alla seguente: ponendo $x = 7m$, l'equazione diofantea

$$40 \cdot 7\ m + 252y = 44$$

ha soluzione? Per rispondere basta controllare se il massimo comune divisore fra $40 \cdot 7 = 280$ e 252 divide o no 44... □

Esercizio 12.17. Trovare tutte le soluzioni intere dell'equazione

$$341x \equiv 15 \quad (912)$$

Esercizio 12.18. Trovare tutte le soluzioni della congruenza

$$18\ x \equiv 1 \quad (25)$$

Quante sono le soluzioni x con $-10 \leq x \leq 300$?

Esercizio 12.19. a) Trovare tutti i numeri interi che risolvono l'equazione

$$70x \equiv 222 \qquad (24)$$

b) Trovare tutti i numeri interi che risolvono l'equazione

$$(x+1)(x+2) \equiv 0 \qquad (24)$$

Esercizio 12.20. Trovare tutte le soluzioni della congruenza

$$12\ x \equiv 33 \quad (57)$$

Quante sono le soluzioni x con $-10 \leq x \leq 10$?

Esercizio 12.21. Trovare tutte le soluzioni della congruenza

$$1008\ x \equiv 12 \quad (11)$$

Esercizio 12.22. a) Trovare tutte le soluzioni della congruenza

$$546x \equiv 442 \qquad (260)$$

b) Trovare tutte le soluzioni della congruenza

$$7x \equiv -46 \qquad (58)$$

c) Trovare le soluzioni comuni alle due equazioni.

Esercizio 12.23. Trovare tutte le soluzioni della congruenza

$$44\ x \equiv 10 \quad (105)$$

Esercizio 12.24. Trovare per quali $b \in \mathbb{Z}$ e $m \in \mathbb{Z}^+$ si può risolvere la congruenza

$$2\ x \equiv b \quad (m)$$

Esercizio 12.25. a) Risolvere la congruenza

$$168x \equiv 3080 \quad (455)$$

b) Per quali valori del numero intero positivo m la congruenza

$$168x \equiv 1540 \quad (35m)$$

ammette soluzione ?

Esercizio 12.26. Trovare tutte le soluzioni della congruenza

$$420\ x \equiv 91 \quad (119)$$

Quante sono le soluzioni x con $-10 \leq x \leq 300$?

Esercizio 12.27. Trovare tutte le soluzioni della congruenza $42x \equiv 6 \bmod 110$ e stabilire il numero delle soluzioni nell'intervallo $[-1000, 2000]$.

Esercizio 12.28. Trovare tutte le soluzioni della congruenza $9x \equiv 3^{15} \bmod 17$.

Esercizio 12.29. Determinare per quali valori del parametro k la congruenza

$$-6x \equiv 20 \bmod 7k$$

ha soluzione e risolverla per $k = 8$.

Esercizio 12.30. a) Calcolare $MCD(3192, 117)$.
b) Trovare tutti gli $m \in \mathbb{Z}$ che soddisfano

$$3192\ m \equiv 288 \mod 117$$

e tali che $0 \leq m \leq 234$.

Esercizio 12.31. Dire se le seguenti proposizioni sono vere o false e motivare la risposta:

a) per tutti i numeri naturali positivi n, $7^n \equiv n^3 + 3n^2 + 2n + 1 \mod 5$.
b) Per tutti i numeri naturali positivi n, $7^n \equiv n^3 + 3n^2 + 2n + 1 \mod 3$.
c) Per tutti i numeri naturali positivi n, $7^n \geq n^3 + 3n^2 + 2n + 1$.

Esercizio 12.32. a) Trovare tutti gli interi x che soddisfano la congruenza:

$$1386x \equiv 1890 \quad (294)$$

b) Trovare tutti gli interi y che soddisfano la congruenza:

$$1386y^2 \equiv 1890 \quad (294)$$

Esercizio 12.33. a) Risolvere la congruenza

$$396x \equiv 234 \quad (1050)$$

b) Per quali valori dell'intero k la congruenza

$$396x \equiv 234 \quad (105 \cdot k)$$

ha soluzione?

Esercizio 12.34. a) Risolvere la congruenza

$$5920x \equiv 160 \quad (504)$$

b) Per quali valori del numero intero positivo m la congruenza

$$5920x \equiv 160 \quad (56m)$$

ammette soluzione ?

ESERCIZIO 12.35. a) Trovare l'insieme $S_1 \subseteq \mathbb{Z}$ delle soluzioni della congruenza lineare:

$$3315\ x \equiv 816 \qquad \text{mod } 952$$

b) Trovare l'insieme $S_2 \subseteq \mathbb{Z}$ delle soluzioni della congruenza lineare:

$$126x \equiv 42 \qquad \text{mod } 77$$

c) Descrivere $S_1 \cap S_2$

ESERCIZIO 12.36. Trovare tutte le soluzioni di

$$x^2 + 1 \equiv 0 \text{ mod } 65$$

ESERCIZIO 12.37. Dimostrare che, per ogni numero primo p esiste un numero naturale n tale che

$$6n^2 + 5n + 1 \equiv 0 \text{ mod } p$$

CAPITOLO 13

Congruenze esponenziali

1. Il piccolo teorema di Fermat

In questa sezione studieremo un importante teorema che riguarda le potenze dei numeri modulo un intero positivo m.

TEOREMA 13.1 (Il piccolo teorema di Fermat). *Se p è un numero primo e a è un numero intero che non è un multiplo di p, allora vale*

$$a^{p-1} \equiv 1 \quad (p)$$

OSSERVAZIONE 13.2. Sia $p = 7$. Il teorema ci garantisce che per ogni $a \in \mathbb{Z}$ che non sia multiplo di 7 vale:

$$a^6 \equiv 1 \quad (7).$$

Avvertiamo subito che può accadere che 6 non sia il più piccolo numero t tale che

$$a^t \equiv 1 \quad (7).$$

Per esempio per $a = 2$ troviamo:

$$2^3 \equiv 1 \quad (7)$$

Invece per $a = 3$ la più piccola potenza che dà un risultato congruo a 1 modulo 7 è effettivamente 6. Infatti le potenze di 3 modulo 7 sono le seguenti:

$$3^1 = 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1$$

Approfondiremo più avanti questa osservazione.

DIMOSTRAZIONE. Dato un intero $a \not\equiv 0 \quad (p)$ consideriamo i numeri

$$a, 2a, \ldots, (p-1)a$$

Questi $p-1$ numeri sono a due a due non congrui fra loro modulo p. Supponiamo infatti, per assurdo, che esistano i e j $(0 \leq i < j \leq p-1)$ tali che $ia \equiv ja \quad (p)$.

Ora sappiamo (per il Teorema 11.27) che a ammette un inverso modulo p. Sia dunque b un inverso di a. Moltiplicando per b otteniamo:

$$iab \equiv jab \quad (p)$$

ossia

$$i \equiv j \quad (p)$$

Poiché avevamo supposto $0 \leq i < j \leq p-1$ abbiamo trovato un assurdo.

Dunque la lista

$$a, 2a, \ldots, (p-1)a$$

comprende $p-1$ numeri i cui resti nella divisione per p sono tutti diversi da 0 e a due a due distinti. Allora i resti dei numeri $a, 2a, \ldots, (p-1)a$ sono esattamente, a meno di riordinarli, i numeri

$$1, 2, \ldots, (p-1)$$

Possiamo dunque scrivere che

$$a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \qquad (p)$$

Questa congruenza, raccogliendo a sinistra i fattori uguali ad a, equivale alla seguente:

$$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \qquad (p)$$

Ora osserviamo che $p-1$ è invertibile modulo p (sempre per il Teorema 11.27), e moltiplichiamo entrambi i membri per un suo inverso. Otteniamo

$$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-2) \equiv 1 \cdot 2 \cdot 3 \cdots (p-2) \qquad (p)$$

Poi moltiplichiamo entrambi i membri per un inverso di $p-2$, e così via..

Alla fine troviamo

$$a^{p-1} \equiv 1 \qquad (p)$$

come volevamo dimostrare. □

Diamo adesso una diversa dimostrazione del piccolo teorema di Fermat dovuta ad Eulero. Per un'altra dimostrazione, consultate anche il Paragrafo 8 del Capitolo 4 di [**?**].

DIMOSTRAZIONE. Per prima cosa dimostriamo che p divide $\binom{p}{i}$ quando $0 < i < p$. Infatti sappiamo che

$$\binom{p}{i} \; i! \; (p-i)! = p!$$

e, per il teorema di decomposizione unica in prodotto di fattori primi, p, che divide il membro di destra, deve dividere il membro di sinistra. Poiché p non può dividere $i!$ $(p-i)!$ (che sono prodotti di numeri positivi strettamente minori di p) possiamo dedurre, per la proprietà caratterizzante dei numeri primi (ossia quella che dice che se p è primo e divide un prodotto ab allora p deve dividere a o p deve dividere b), che p deve dividere $\binom{p}{i}$.

A questo punto possiamo osservare che, dati due numeri interi a e b, lo sviluppo del binomio $(a+b)^p$ ha, modulo p, una scrittura molto semplificata. Infatti vale

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} \equiv a^p + b^p \qquad (p)$$

dato che, appunto, p divide tutti i coefficienti $\binom{p}{i}$ $(0 < i < p)$.

In particolare, nel caso $b = 1$, abbiamo

$$(a+1)^p \equiv a^p + 1 \qquad (p)$$

Ora proviamo che, per ogni $a \in \mathbb{Z}$ vale

$$a^p \equiv a \quad (p)$$

Questa relazione, nel caso in cui a non è multiplo di p, ci dà (dividendo per a) l'enunciato del teorema.

Ci basta dimostrare che, per ogni $a \in \mathbb{N}$,

$$a^p \equiv a \quad (p)$$

(il caso dei numeri negativi si ricava poi immediatamente).

Lo dimostriamo per induzione su a.

Il caso base, per $a = 0$,

$$0^p \equiv 0 \quad (p)$$

è banale.

Supponiamo ora che questa relazione sia vera fino ad $a = n$ e proviamo a dimostrare che

$$(n+1)^p \equiv n+1 \quad (p)$$

(se ci riusciamo la nostra dimostrazione è terminata).

Ora, per quanto visto sopra possiamo scrivere che

$$(n+1)^p \equiv n^p + 1 \quad (p)$$

Ma, per ipotesi induttiva, $n^p \equiv n \quad (p)$ per cui

$$(n+1)^p \equiv n+1 \quad (p)$$

□

Mostriamo nel seguente esempio una importante applicazione del piccolo teorema di Fermat al calcolo veloce di potenze modulo un numero primo.

Esempio 13.3. Se vogliamo calcolare

$$15^{1443} \equiv ? \quad (17)$$

possiamo utilizzare il piccolo teorema di Fermat che ci dice che

$$15^{16} \equiv 1 \quad (17)$$

Ora $1443 = 16 \cdot 90 + 3$ dunque

$$15^{1443} \equiv (15^{16})^{90}\, 15^3 \equiv 1^{90}\, 15^3 \quad (17)$$

Ma $15 \equiv -2 \quad (17)$ dunque

$$15^{1453} \equiv (-2)^3 \equiv -8 \equiv 9 \quad (17)$$

Esempio 13.4. Attenzione, se il modulo non è primo, l'enunciato del piccolo teorema di Fermat non vale più: non è vero, per esempio, che $2^5 \equiv 1 \quad (6)$. Infatti

$$2^5 = 32 \equiv 2 \quad (6)$$

Dal piccolo teorema di Fermat si ricava subito questo corollario:

Corollario 13.5. *Se p è un numero primo, per ogni numero intero a vale*

$$a^p \equiv a \quad (p)$$

Dimostrazione. Se a non è multiplo di p per il piccolo teorema di Fermat vale

$$a^{p-1} \equiv 1 \quad (p)$$

da cui si ottiene la tesi moltiplicando per a entrambi i membri. È poi immediato verificare che se $a \equiv 0 \quad (p)$ allora la tesi è vera.

□

Questo ci dà un criterio per decidere se un numero non è primo:

Corollario 13.6. *Se $n > 1$ è un numero intero tale che per qualche numero intero a vale*

$$a^n \not\equiv a \quad (n)$$

allora n non è primo.

Dimostrazione. Si tratta della contronominale del corollario precedente. □

È interessante capire se con questi ragionamenti si può trovare un criterio per dire con certezza se un numero è primo (non solo per dire se un numero NON è primo). Saremmo infatti tentati di pensare che se prendiamo un numero intero $n > 1$ e scopriamo che per tutti i numeri interi a vale

$$a^n \equiv a \quad (n)$$

allora n è primo. Questo non è vero: ci sono infiniti numeri che soddisfano questa proprietà ma non sono primi. Si chiamano *numeri di Carmichael*[1] o *falsi primi*.

Esercizio 13.7. Dimostrare che 561 è un numero di Carmichael (è il più piccolo esistente).

Esercizio 13.8. Dimostrare che 1105 e 1729 sono numeri di Carmichael (sono il secondo e il terzo nella lista dei numeri di Carmichael).

2. Un interessante risvolto applicativo: il metodo di crittografia RSA

Consideriamo due numeri primi distinti p e q, e prendiamo un numero e che sia primo con $(p-1)(q-1)$. Sappiamo dunque che e è invertibile modulo $(p-1)(q-1)$, e chiamiamo d un suo inverso.

La seguente semplice proposizione è il cuore del metodo di crittografia che vogliamo descrivere:

Proposizione 13.9. *Dati p, q, e, d come sopra, per ogni numero m con $0 \leq m < pq$ vale*

$$(m^e)^d \equiv m \quad (pq)$$

Dimostrazione. Osserviamo che per il teorema cinese del resto l'equazione

$$x \equiv m \quad (pq)$$

è equivalente al sistema

$$\begin{cases} x \equiv m & (p) \\ x \equiv m & (q) \end{cases}$$

Dunque ci basta dimostrare che $(m^e)^d$ è una soluzione del sistema.

Verifichiamo che $(m^e)^d$ è soluzione della prima equazione (per la seconda equazione si procederà in maniera del tutto analoga), ossia verifichiamo che è vera la congruenza:

$$(m^e)^d \equiv m \quad (p)$$

Ora, se $p|m$ la congruenza appena scritta diventa $0 \equiv 0 \quad (p)$ che è vera.

Se invece $p \nmid m$ allora possiamo applicare il piccolo teorema di Fermat. Infatti per costruzione

$$ed \equiv 1 \qquad ((p-1)(q-1))$$

dunque possiamo scrivere

$$ed = 1 + k(p-1)(q-1)$$

per un certo intero k.

Allora

$$(m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \cdot 1^{k(q-1)} \equiv m \quad (p)$$

dove abbiamo usato il piccolo teorema di Fermat per dire che $m^{p-1} \equiv 1 \quad (p)$.

□

[1] Robert Carmichael, matematico americano,1878-1967.

Nel 1977 Ronald Rivest, Adi Shamir e Leonard Adleman inventarono un metodo (detto RSA dalle iniziali dei loro cognomi) per scambiarsi messaggi criptati il cui funzionamento può essere schematicamente riassunto nel seguente modo.[2]

Supponiamo che A voglia inviare un messaggio segreto a B (non occorre pensare a chissà quali contesti di spionaggio e controspionaggio, A per esempio potremmo essere noi mentre digitiamo il codice della nostra carta di credito per fare un acquisto online).

Innanzitutto B ha scelto due numeri primi distinti p e q molto grandi (attualmente si scelgono numeri di circa trecento cifre: osserviamo che la ricerca di numeri primi grandi è un problema matematico di per sé interessante, che ha dunque anche una importante applicazione).

Visto che conosce p e q, B conosce anche $p-1$ e $q-1$ e può dunque facilmente scegliere e e d con le caratteristiche illustrate in questo paragrafo.

A questo punto B consegna ad A i numeri pq ed e. Anzi, li può addirittura rendere pubblici, in modo che altri possano inviargli messaggi crittati, non solo A.

Quando A vuole inviare un messaggio, questo messaggio può essere facilmente codificato da un numero m con $0 < m < pq$ (se è un messaggio numerico è già un numero, se è un messaggio con lettere, si può certo trovare un modo di associare ad ogni lettera un numero, dunque il messaggio finale risulterà un numero m, magari molto grande, ottenuto scrivendo uno accanto all'altro tutti i numeri che rappresentano le lettere).[3]

A questo punto A non invia il numero m, ma calcola m^e modulo pq e invia dunque un numero c con $0 < c < pq$ e $c \equiv m^e \pmod{pq}$.

Dunque B riceve il messaggio c. Per decodificarlo calcolerà c^d modulo pq e, per la Proposizione 13.9, ritroverà il messaggio originale m.

Come mai questo sistema è efficace? Ricordiamo che solo B conosce il numero d, e il punto è proprio questo. Il numero d è stato ricavato da e e dalla conoscenza dei numeri $p-1$ e $q-1$, mentre sono pubblici solo i numeri e e il **prodotto** pq. Per ricavare $p-1$ e $q-1$ conoscendo il prodotto pq bisognerebbe saper fattorizzare pq, e questa è una operazione che, al giorno d'oggi, con numeri così grandi, non è possibile eseguire in tempo utile. E non esiste per il momento neppure nessun altro metodo che permetta, dato un numero c che sappiamo essere congruo modulo pq ad una potenza e-esima di un certo numero ignoto, di ritrovare in tempo utile questo numero ignoto.[4]

Nelle poche righe precedenti abbiamo descritto in maniera schematica il metodo RSA, senza discutere le molte accortezze tecniche che occorre usare nella pratica, che non competono a questo corso ma ad un corso di crittografia. Ad ogni modo, una volta che viene applicato con tutte le accortezze del caso, il metodo RSA è ritenuto molto affidabile.

Abbiamo fatto solo un primo accenno alle complesse problematiche della crittografia, ma per voi che intraprendete la carriera di matematici può essere interessante sapere che un teorema di aritmetica elementare, semplice ma profondo, come il piccolo teorema di Fermat, ha ripercussioni applicative così importanti.

---

[2]Per coloro che sono interessati ad una introduzione divulgativa (non tecnica) alla storia della crittografia fin dalle origini, segnalo il libro di S. Singh *Codici e Segreti*.

[3]Ricordiamo che pq è molto grande, dunque c'è spazio per codificare anche messaggi molto lunghi. Altrimenti A dovrà spezzare il suo messaggio e inviare vari numeri m_1, m_2 etc...

[4]Se siete curiosi potete dare un'occhiata all'articolo di Rivest e Kaliski *RSA problem*, https://people.csail.mit.edu/rivest/RivestKaliski-RSAProblem.pdf

3. Le classi di resto modulo un intero positivo. Struttura additiva e moltiplicativa.

Cominciamo con un esempio. Consideriamo i possibili resti della divisione euclidea di un numero intero per 10. Abbiamo 10 possibilità: resto uguale a 0,1,2,3,. . . , 9. Quali sono i numeri che danno resto 1? Eccone alcuni: 1,11,21,31,. . . ....-9,-19,-29,-39, -49. . .

Chiamiamo $[1]_{10}$ l'insieme costituito da questi numeri:

$$[1]_{10} = \{x \in \mathbb{Z} \mid x \equiv 1 \quad (10)\}$$

Analogamente, chiamiamo $[2]_{10}$ l'insieme dei numeri interi la cui divisione per 10 dà resto 2, e in generale, per $i = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, chiamiamo $[i]_{10}$ l'insieme dei numeri interi la cui divisione per 10 dà resto i.

Gli insiemi $[0]_{10}$, $[1]_{10}$, $[2]_{10}$,. . . , $[9]_{10}$ si chiamano "classi di resto modulo 10"; la loro unione è uguale a tutto $\mathbb{Z}$ giacché ogni numero intero appartiene ad una (e ad una sola) delle classi. Chiamiamo ora $\mathbb{Z}_{10}$ l'insieme i cui elementi sono tutte le classi di resto modulo 10:

$$\mathbb{Z}_{10} = \{[0]_{10}, [1]_{10}, \ldots, [9]_{10}\}$$

Possiamo arricchire questo insieme definendo due operazioni, una somma e una moltiplicazione.

Prima estendiamo la nostra notazione: fin qui per esempio non abbiamo definito il simbolo $[11]_{10}$. Infatti abbiamo preso in considerazione solo simboli in cui fra le parentesi quadre c'è un resto 0,1,. . . , 9 di una divisione euclidea per 10. Decidiamo di accettare anche $[11]_{10}$ intendendo che $[11]_{10} = [1]_{10}$. E anche, per esempio, $[127]_{10} = [7]_{10}$. Insomma ci mettiamo d'accordo di poter indicare una classe di resto $[i]_{10}$ anche col simbolo $[s]_{10}$ dove s è un qualunque numero intero tale che

$$s \equiv i \quad (10)$$

Ora siamo pronti a definire la somma e la moltiplicazione di elementi di $\mathbb{Z}_{10}$. Poniamo:

$$[a]_{10} \cdot [b]_{10} = [ab]_{10}$$

$$[a]_{10} + [b]_{10} = [a + b]_{10}$$

Per esempio:

$$[7]_{10} \cdot [5]_{10} = [35]_{10} = [5]_{10}$$

$$[6]_{10} + [8]_{10} = [14]_{10} = [4]_{10}$$

Insomma in $\mathbb{Z}_{10}$ "sette" per "cinque" fa "cinque" e "sei" più "otto" fa "quattro".

In realtà, per essere sicuri di aver definito una buona somma e una buona moltiplicazione, bisogna verificare che, se

$$[a]_{10} = [a']_{10}$$

$$[b]_{10} = [b']_{10}$$

allora

$$[a]_{10} \cdot [b]_{10} = [a']_{10} \cdot [b']_{10}$$

$$[a]_{10} + [b]_{10} = [a']_{10} + [b']_{10}$$

insomma che queste operazioni non dipendono dai numeri a e b che mettiamo fra parentesi quadre ma solo dalle loro classi di resto.

Esercizio 13.10. Fate questa verifica. (Suggerimento: visto che $[a]_{10} = [a']_{10}$ allora sarà $a' = a+10k$ e analogamente $b' = b+10t$. Dunque per esempio, per quel che riguarda la moltiplicazione, vale $[a']_{10} \cdot [b']_{10} = [(a+10k)(b+10t)]_{10} = [ab+10bk+10at+100kt]_{10} = [ab]_{10} = [a]_{10}[b]_{10}$.)

Con queste operazioni l'insieme $\mathbb{Z}_{10}$ diventa un "anello commutativo con unità". Discuteremo la definizione formale di anello (anche se la avete già vista a Geometria 1) in uno dei prossimi capitoli.

Intanto osserviamo che la somma e la moltiplicazione che abbiamo definito hanno molte delle buone proprietà a cui "siamo abituati" dalla moltiplicazione e dalla somma in $\mathbb{Z}$ (proprietà commutativa e associativa di entrambe le operazioni, proprietà distributive, esistenza dell'elemento neutro per entrambe operazioni, esistenza dell'opposto rispetto alla somma..).

C'è però una cosa nuova in $\mathbb{Z}_{10}$, rispetto a $\mathbb{Z}$. Vale infatti

$$[2]_{10} \cdot [5]_{10} = [10]_{10} = [0]_{10}$$

ossia il prodotto di due elementi diversi da $[0]_{10}$ ha come risultato $[0]_{10}$ (mentre in $\mathbb{Z}$ il prodotto di due interi diversi da zero è sempre diverso da 0). Si dice a questo proposito che $[2]_{10}$ e $[5]_{10}$ sono due *divisori dello zero* in $\mathbb{Z}_{10}$.

Passiamo al caso generale. Sia m un numero intero positivo.
Per ogni $i = 0, 1, 2, \ldots, m-1$ chiamiamo $[i]_m$ la "classe di resto di i modulo m", ossia l'insieme dei numeri che danno resto i quando si considera la loro divisione euclidea per m:

$$[i]_m = \{x \in \mathbb{Z} \mid x \equiv i \pmod{m}\}$$

Come nell'esempio in cui $m = 10$, osserviamo che l'unione di tutte le classi di resto modulo m dà tutto $\mathbb{Z}$.
Chiamiamo $\mathbb{Z}_m$ l'insieme di tutte le classi di resto modulo m:[5]

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Si tratta dunque un insieme di cardinalità m.

Come sopra adottiamo la convenzione per cui possiamo indicare la classe $[i]_m$ anche col simbolo $[s]_m$ dove s è un qualunque numero intero tale che

$$s \equiv i \pmod{m}$$

Per esempio, con $m = 37$:

$$[5]_{37} = [42]_{37} = [412]_{37}$$

Possiamo allora definire la somma e la moltiplicazione di elementi di $\mathbb{Z}_m$:

$$[a]_m \cdot [b]_m = [ab]_m$$

$$[a]_m + [b]_m = [a+b]_m$$

Anche questa volta si verifica (fate di nuovo il facile esercizio!) che queste operazioni sono ben definite e che non dipendono dai numeri a e b ma solo delle loro classi di resto, e $\mathbb{Z}_m$ risulterà un anello commutativo con unità.

[5] In vari testi, come [?], trovate questo insieme indicato con il simbolo $\mathbb{Z}/m\mathbb{Z}$.

4. Esercizi

Esercizio 13.11. a) Trovare il numero naturale m tale che $0 \leq m < 13$ e

$$[2^{(2^{10})}]_{13} = [m]_{13}$$

b) Trovare il numero naturale k tale che $0 \leq k < 3$ e

$$[(138139140141 \ldots 999)^{1987} - 1]_3 = [k]_3$$

Esercizio 13.12. Consideriamo la funzione $g : \mathbb{Z}_5 \times \mathbb{Z}_5 \to \mathbb{Z}_5 \times \mathbb{Z}_5$ che è definita dalla seguente relazione:

$$\forall\, [a],\ [b] \in \mathbb{Z}_5, \quad g(([a],[b])) = ([a-3b],[a+3b])$$

Dire se g è iniettiva, surgettiva, bigettiva.

Esercizio 13.13. a) Trovare l'insieme delle soluzioni della congruenza lineare:

$$327\ x \equiv 416 \qquad \mod (52)$$

b) Dire se la funzione $f : \mathbb{Z}_{52} \to \mathbb{Z}_{52}$ data da

$$f([x]) = [15x]$$

è iniettiva, surgettiva, bigettiva.

Esercizio 13.14 (Teorema di Wilson[6]). Dimostrare che, se p è primo, vale

$$(p-1)! \equiv -1 \qquad (p)$$

Se invece m è un numero non primo, la congruenza

$$(m-1)! \equiv -1 \qquad (m)$$

è vera o falsa?

Esercizio 13.15. Dimostrare che, per ogni $n \in \mathbb{N} - \{0\}$, $17^{16^n} \equiv 4 \mod 7$.

Esercizio 13.16. a) Quante sono tutte le possibili funzioni $f : \mathbb{Z}_{15} \to \mathbb{Z}_{20}$?
b) Quanti sono gli elementi invertibili di $\mathbb{Z}_{15}$? E quelli invertibili di $\mathbb{Z}_{20}$?
c) Quante sono le funzioni $g : \mathbb{Z}_{15} \to \mathbb{Z}_{20}$ che mandano elementi invertibili di $\mathbb{Z}_{15}$ in elementi invertibili di $\mathbb{Z}_{20}$?
d) Quante sono le funzioni iniettive $h : \mathbb{Z}_{15} \to \mathbb{Z}_{20}$ che mandano elementi invertibili di Z_{15} in elementi invertibili di $\mathbb{Z}_{20}$?

Esercizio 13.17. Dimostrare che esiste un multiplo di 174 nella cui scrittura decimale appare solo la cifra 6.

[Traccia: $174 = 6 \cdot 29$. C'è un n tale che il numero 66666...66 (il 6 compare n volte) sia divisibile per 174 ? Basta scoprire quando il numero 11111...11 (l'1 compare n volte) è divisibile per 29. Ora, $11111...11 = 1 + 10 + 10^2 + \cdots + 10^{n-1} = \frac{10^n-1}{10-1}$...]

Esercizio 13.18. Qual è l'ultima cifra del numero 3^{13452} scritto in base 10? E del numero 6^{245389}?

Esercizio 13.19. Dimostrare che, per ogni numero naturale n, $n(n^6-1)$ è divisibile per 42.

Esercizio 13.20. Dimostrare che, per ogni intero positivo n, $2^{3n+3} - 7n - 8$ è divisibile per 49.

[6]John Wilson, matematico inglese, 1741-1793.

Esercizio 13.21. Dimostrare che non esiste nessuna funzione $f : \mathbb{N} \to \mathbb{N}$ tale che, per ogni $n \in \mathbb{N}$

$$f(f(n)) = n + 2015$$

Esiste una simile funzione se nella formula precedente si sostituisce 2015 con 2016 ?

CAPITOLO 14

Teorema di Eulero

1. Gruppi e sottogruppi: prime proprietà

Cominciamo subito scrivendo la definizione formale di gruppo (la avete in realtà già vista a Geometria 1).

DEFINIZIONE 14.1. Un *gruppo* G è un insieme non vuoto dotato di una operazione che ad ogni coppia di elementi $a, b \in G$ associa un elemento di G indicato con $a \cdot b$ e ha le seguenti proprietà:

(1) dati $a, b, c \in G$ vale $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (proprietà associativa);
(2) esiste un elemento $e \in G$ tale che $a \cdot e = e \cdot a = a$ per ogni $a \in G$ (esistenza dell'elemento neutro, detto anche identità, in G);
(3) per ogni $a \in G$ esiste un elemento $a^{-1} \in G$ tale che $a \cdot a^{-1} = a^{-1} \cdot a = e$ (esistenza dell'inverso in G).

Un gruppo si dice *commutativo* o *abeliano*[1] se, per ogni $a, b \in G$ vale $a \cdot b = b \cdot a$. Un gruppo G si dice finito se l'insieme G ha cardinalità finita.

ESEMPIO 14.2. Ecco due esempi di gruppi non commutativi.

Consideriamo un insieme con n elementi X. L'insieme $Bij(X, X)$ delle funzioni bigettive da X in X è un gruppo con $n!$ elementi, chiamato S_n, con l'operazione data dalla composizione fra funzioni. Fate fin d'ora la verifica che S_n è un gruppo, e dimostrate anche che non è commutativo se $n \geq 3$. Studieremo più avanti S_n in maniera più approfondita.

Se considerate l'insieme $Mat_{n\times n}(K)^*$ delle matrici $n \times n$ *invertibili* a coefficienti in un campo K, noterete che $Mat_{n\times n}(K)^*$ è un gruppo rispetto all'operazione di prodotto fra matrici. Anche in questo caso si tratta di un gruppo non commutativo (se $n \geq 2$).

ESEMPIO 14.3. Ecco altri esempi, e controesempi, familiari.

L'insieme $\mathbb{Z}$ considerato con l'operazione $+$ è un gruppo commutativo infinito; rispetto alla moltiplicazione, invece, non è un gruppo perché solo gli elementi 1 e -1 hanno un inverso. L'insieme $\mathbb{N}$ non è un gruppo né con l'addizione né con la moltiplicazione. I campi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, sono gruppi commutativi rispetto all'addizione, mentre gli insiemi $\mathbb{Q}-\{0\}$, $\mathbb{R}-\{0\}$,$\mathbb{C}-\{0\}$ sono gruppi commutativi rispetto alla moltiplicazione.

Ogni spazio vettoriale V è un gruppo commutativo rispetto alla addizione.

D'ora in avanti, quando parleremo di un gruppo, ometteremo, tutte le volte che sarà possibile farlo senza creare ambiguità, il simbolo $\cdot$ per la moltiplicazione; scriveremo dunque ab invece di $a \cdot b$, $a^2 = aa$ invece di $a \cdot a$. Inoltre nel fare il prodotto fra n elementi del gruppo scriveremo spesso $a_1 \cdot a_2 \cdots a_n$ omettendo le parentesi, visto che vale la proprietà associativa (una facile induzione su n ci mostra che il risultato del prodotto non dipende da come erano collocate le parentesi).

[1] In onore di Niels Henrik Abel, matematico norvegese, 1802-1829.

Il seguente teorema, semplice ma importante, mette in luce alcune prime proprietà dei gruppi che derivano immediatamente dalla definizione.

TEOREMA 14.4. *Dimostrare che, se G è un gruppo, allora*

(1) *C'è un solo elemento neutro e.*
(2) *Per ogni $a \in G$ c'è un unico inverso di a.*
(3) *Per ogni $a \in G$ vale $(a^{-1})^{-1} = a$.*
(4) *Per ogni $a, b \in G$ vale $(ab)^{-1} = b^{-1}a^{-1}$.*
(5) *Siano a, b, c elementi di G. Allora l'equazione $axb = c$ ha un'unica soluzione $x = a^{-1}cb^{-1}$ in G.*

DIMOSTRAZIONE.
(1) Supponiamo che ci siano due elementi neutri e ed e'. Allora possiamo scrivere, che $e = ee' = e'$ dove per il primo $=$ abbiamo sfruttato la proprietà di elemento neutro di e' (abbiamo infatti moltiplicato a destra per e') e per il secondo $=$ abbiamo sfruttato la proprietà di elemento neutro di e (abbiamo moltiplicato e' a sinistra per e).
(2) Siano h e k due inversi di a. Allora

$$h = he = h(ak) = (ha)k = ek = k$$

(3) Osserviamo che $(g^{-1})^{-1}g^{-1} = g^{-1}(g^{-1})^{-1} = e$ per definizione di $(g^{-1})^{-1}$. Ma sappiamo anche che $gg^{-1} = g^{-1}g = e$ per definizione di g^{-1}. Dunque osserviamo che sia g sia $(g^{-1})^{-1}$ sono inversi di g^{-1}. Per l'unicitàà dell'inverso stabilita nel punto (2) possiamo concludere che $g = (g^{-1})^{-1}$.
(4) Basta verificare che $b^{-1}a^{-1}$ è un inverso di ab. Lo faremo moltiplicandolo a sinistra (la dimostrazione moltiplicandolo a destra è analoga).

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$$

dove abbiamo usato in maniera sostanziale la proprietà associativa.
(5) Un elemento $\overline{x}$ soddisfa l'equazione $axb = c$ se e solo se vale $a\overline{x}b = c$. Questa uguaglianza è vera se e solo se è vera $\overline{x}b = a^{-1}c$, come si vede moltiplicando ognuno dei due membri, a sinistra, per a^{-1}. Moltiplicando ognuno dei due membri, a destra, per b^{-1} si vede che questa uguaglianza a sua volta è vera se e solo se è vera $\overline{x} = a^{-1}cb^{-1}$. Dunque le soluzioni della equazione $axb = c$ coincidono con le soluzioni della equazione $x = a^{-1}cb^{-1}$, che, come si vede, sono una sola, ossia $a^{-1}cb^{-1}$.

□

Fra i sottoinsiemi di G rivestono un ruolo particolare quelli che, rispetto all'operazione $\cdot$, sono a loro volta dei gruppi:

DEFINIZIONE 14.5. Un *sottogruppo* H di un gruppo G è un sottoinsieme di G che soddisfa le tre seguenti proprietà:

(1) $e \in H$
(2) $a, b \in H \Rightarrow ab \in H$
(3) $a \in H \Rightarrow a^{-1} \in H$

Per indicare che H è un sottogruppo di G si scrive $H < G$.

OSSERVAZIONE 14.6. In particolare, fra i sottogruppi di un gruppo G ci sono sempre G stesso e il sottogruppo banale $\{e\}$.

Indichiamo subito un importante sottogruppo:

DEFINIZIONE 14.7 (Centro di un gruppo). Dato un gruppo G si chiama *centro* di G il sottoinsieme formato dagli elementi che commutano con tutti gli elementi del gruppo:

$$Z(G) = \{g \in G \mid gh = hg \quad \forall h \in G\}$$

ESERCIZIO 14.8. Dimostrare che $Z(G)$ è un sottogruppo di G.

Si osserva subito che se il gruppo G è abeliano allora $Z(G) = G$.

ESEMPIO 14.9. Sia a un elemento di un gruppo G. Consideriamo il sottoinsieme di G

$$(a) = \{a^i \mid i \in \mathbb{Z}\}$$

Spieghiamo bene la notazione. Se $s > 0$ con a^s si intende, come immaginate, il prodotto di a per se stesso s volte. Poi si pone $a^0 = e$. Inoltre se $i > 0$ e scriviamo a^{-i} intendiamo $(a^{-1})^i$. Per il punto (4) del Teorema 14.4 questo è uguale a $(a^i)^{-1}$ (per esempio $a^{-2} = a^{-1}a^{-1} = (a^2)^{-1}$). Il sottoinsieme (a) è un sottogruppo di G e si chiama *sottogruppo ciclico generato da* a.

I sottogruppi ciclici di $\mathbb{Z}$ (con l'operazione $+$) sono, al variare di $m \in \mathbb{Z}$, i sottogruppi

$$(m) = \{km \mid k \in \mathbb{Z}\}$$

che coincidono, usando la notazione della scorsa lezione, con le classi di resto $[0]_m$.

DEFINIZIONE 14.10. Se, per qualche $a \in G$ vale $G = (a)$ allora si dice che G è un *gruppo ciclico*.

2. Laterali destri di un sottogruppo. Il Teorema di Lagrange. Ordine di un elemento

DEFINIZIONE 14.11. Sia G un gruppo, H un sottogruppo di G. Chiameremo H-*laterale destro*, o *laterale destro di* H, o *classe laterale destra di* H, un sottoinsieme di G del tipo:

$$gH = \{gh \mid h \in H\}$$

dove $g \in G$.

L'insieme i cui elementi sono gli H-laterali destri si indica con G/H e la sua cardinalità $|G/H|$ si chiama *indice* di H in G.

In particolare osserviamo che $eH = H$ ossia H è un particolare H-laterale destro. A parte questo caso, i laterali destri di H non sono sottogruppi (come potete facilmente verificare nel caso in cui $G = \mathbb{Z}$ con l'operazione $+$ e $H = (m)$ per un certo intero positivo m), ma solo sottoinsiemi di G.

Gli H laterali destri forniscono però una partizione di G, ossia G è unione disgiunta dei suoi laterali destri, come mostra la seguente:

TEOREMA 14.12. *Ogni elemento w di G è contenuto in uno e un solo H-laterale destro: wH.*

DIMOSTRAZIONE. Osserviamo subito che $w \in wH$ visto che $e \in H$ e allora $w = we \in wH$. Supponiamo ora che w appartenga anche al laterale γH, dove $\gamma \in G$. Allora $w = \gamma h_1$ per un certo $h_1 \in H$. Ora osserviamo che il laterale wH e il laterale γH coincidono. Infatti:

$$\gamma H = \{\gamma h \mid h \in H\} = \{\gamma h_1 h \mid h \in H\} = \{wh \mid h \in H\} = wH$$

Il secondo $=$, quello in blu, va spiegato bene. Il punto è che, al variare di h, gli elementi $h_1 h$ descrivono tutti gli elementi del gruppo H: infatti ogni elemento h_2 appartenente ad

H può essere ottenuto come $h_1(h_1^{-1}h_2)$, dove $h_1^{-1}h_2$ appartiene ad H visto che H è un sottogruppo. □

Osservazione 14.13. Illustriamo la proposizione precedente nel caso in cui $G = \mathbb{Z}$ con l'operazione $+$ e $H = (12)$. Il numero 5 appartiene al laterale $5 + (12)$ che, se ci si pensa, è l'insieme che nella lezione scorsa abbiamo chiamato $[5]_{12}$, la classe (laterale) di resto di 5 modulo 12. Ora 5 appartiene anche al laterale $17 + (12)$ ma si verifica subito che i laterali $5 + (12)$ e $17 + (12)$ coincidono (questo è in accordo con la convenzione che avevamo scelto per cui $[5]_{12} = [17]_{12}$).

In conclusione abbiamo una partizione di $\mathbb{Z}$ in unione disgiunta delle seguenti classi laterali:

$$[0]_{12}, [1]_{12}, [2]_{12}, \ldots, [10]_{12}, [11]_{12}$$

Segue dal precedente teorema che due laterali gH e bH o sono disgiunti o coincidono. Il seguente corollario illustra la situazione:

Corollario 14.14. *Dato un laterale gH, si consideri un laterale bH. Allora bH coincide con gH se e solo se $b \in gH$. Altrimenti i due laterali sono disgiunti.*

Dimostrazione. Se $b \in gH$ allora c'è un elemento in comune fra i due laterali. Dunque poiché sappiamo dal Teorema 14.12 che ogni elemento appartiene ad un solo laterale, questo vuol dire che $gH = bH$. Viceversa, se $bH = gH$ allora è immediato concludere che $b \in bH = gH$. □

Svolgete anche l'Esercizio 14.37 che presenta i laterali come classi di equivalenza rispetto ad una relazione.

La partizione di G in unione disgiunta di classi laterali rispetto ad un sottogruppo H ha una importante conseguenza per quel che riguarda le cardinalità, nel caso in cui G sia finito:

Teorema 14.15 (Teorema di Lagrange[2]). *Se G è un gruppo finito e H è un sottogruppo di G allora $|H|$ divide $|G|$.*

Dimostrazione. Visto che G è finito, G è l'unione disgiunta di un numero finito, diciamo n_H, di laterali destri di H. Se dimostriamo che ogni laterale ha cardinalità esattamente $|H|$ allora risulta $|G| = n_H\ |H|$ e dunque $|H|$ divide $|G|$.

Contiamo allora quanti elementi ha il laterale gH, per un qualunque $g \in G$. Visto che gli elementi della forma gh ottenuti al variare di $h \in H$ sono tutti diversi fra loro (se vale $gh_1 = gh_2$ allora moltiplicando a sinistra per g^{-1} abbiamo $h_1 = h_2$), vale che $|gH| = |H|$. □

Segnaliamo subito un importante corollario del Teorema di Lagrange.

Definizione 14.16. Dato un elemento x di un gruppo G, se esiste un minimo intero positivo n tale che $x^n = e$ allora n si indica con $o(x)$ e si chiama *ordine* di x. Se un tale n non esiste allora si dice che x ha ordine infinito e si scrive $o(x) = \infty$.

Corollario 14.17. *In un gruppo finito G, ogni elemento x ha ordine finito e tale ordine $o(x)$ divide $|G|$.*

Dimostrazione. Consideriamo le potenze positive di x di G: $x, x^2, \cdots, x^k, \ldots$. In questa lista ad un certo punto deve comparire e. Infatti, se $x = e$ non c'è nulla da dimostrare. Se $x \neq e$, visto che le potenze sono infinite ma gli elementi del gruppo sono

[2]Joseph-Louis Lagrange, nato Giuseppe Lodovico Lagrangia, matematico italiano, 1736-1813.

finiti, ad un certo punto deve valere $x^i = x^j$ con $1 \leq i < j$. Allora, moltiplicando per l'inverso di x^i, si ottiene $x^{j-i} = e$.

Sia ora $o(x)$, come abbiamo definito sopra, il più piccolo n per cui $x^n = e$ e consideriamo gli elementi

$$\{e, x, x^2, \ldots, x^{o(x)-1}\}$$

Tali elementi sono tutti distinti: se fosse $x^i = x^j$ con $1 \leq i < j \leq o(x)$ allora varrebbe $x^{j-i} = e$ ma questo non è possibile perché $j - i < o(x)$.

Inoltre osserviamo che $\{e, x, x^2, \ldots, x^{o(x)-1}\}$ coincide con il sottogruppo ciclico (x) generato da x (infatti si nota che $x^{-1} = x^{o(x)-1}$, $x^{-2} = x^{o(x)-2}$ etc...e si verifica subito che tutte le potenze di x e di x^{-1} sono presenti nella lista, visto che si ripetono ciclicamente).

Dunque la cardinalità del sottogruppo (x) è uguale a $o(x)$, e dal Teorema di Lagrange si ricava che $o(x)$ divide $|G|$.

□

COROLLARIO 14.18. *Se x è un elemento di un gruppo finito G vale*

$$x^{|G|} = e.$$

DIMOSTRAZIONE. Infatti per il corollario precedente possiamo scrivere $|G| = k \cdot o(x)$ per un certo intero k. Da questo segue che

$$x^{|G|} = x^{k \cdot o(x)} = \left(x^{o(x)}\right)^k = e^k = e$$

□

3. Una prima applicazione: la funzione di Eulero e il Teorema di Eulero.

Il Teorema di Lagrange e il Corollario 14.17 hanno una immediata applicazione aritmetica. Fissato un numero intero positivo m, consideriamo infatti l'anello $\mathbb{Z}_m$. È immediato verificare che gli elementi invertibili di $\mathbb{Z}_m$ costituiscono un gruppo *rispetto alla moltiplicazione*. Tale gruppo viene indicato con la notazione $\mathbb{Z}_m^*$.

ESEMPIO 14.19. Se p è un numero primo, $\mathbb{Z}_p^*$ ha $p - 1$ elementi, visto che tutte le classi (eccetto la [0]) sono invertibili.

Il gruppo Z_{10}^* ha 4 elementi: [1],[3],[7],[9].

Il gruppo Z_{15}^* ha 8 elementi: [1], [2], [4], [7], [8], [11], [13], [14].

DEFINIZIONE 14.20. *La funzione ϕ di Eulero* è la funzione $\phi : \mathbb{N}^{>0} \to \mathbb{N}^{>0}$ definita ponendo $\phi(1) = 1$ e, per $n > 1$,

$$\phi(n) = \text{numero degli interi positivi minori di } n \text{ e primi con } n$$

Dunque la cardinalità di $\mathbb{Z}_m^*$ è uguale a $\phi(m)$. Questo ci permette già di enunciare un teorema che generalizza il piccolo teorema di Fermat:

TEOREMA 14.21. *Fissato un intero positivo m, se a è un intero primo con m vale:*

$$a^{\phi(m)} \equiv 1 \bmod m$$

DIMOSTRAZIONE. Visto che a ed m sono coprimi, sappiamo che $[a]$ appartiene a $\mathbb{Z}_m^*$. Per il Corollario 14.18 in $\mathbb{Z}_m^*$ vale

$$[a]^{\phi(m)} = [1]$$

che equivale a

$$a^{\phi(m)} \equiv 1 \bmod m$$

□

Osservazione 14.22. Se $m = p$ è primo ritroviamo l'enunciato del piccolo teorema di Fermat, visto che $\phi(p) = p-1$ (abbiamo dunque dato, tramite il Teorema di Lagrange, un'altra dimostrazione del piccolo teorema di Fermat). In questo caso, come vedremo più avanti, vale anche che $\mathbb{Z}_p^*$ è un gruppo ciclico, ossia esiste un elemento in $\mathbb{Z}_p^*$ di ordine esattamente $p-1$.

Osservazione 14.23. Avremmo potuto dimostrare il Teorema 14.21 anche imitando la dimostrazione del piccolo teorema di Fermat nel caso dei gruppi abeliani finiti, come suggerito dall'Esercizio 14.32. Ma abbiamo preferito introdurre subito il Teorema di Lagrange, che ha valore più generale, e i laterali, che avranno anch'essi grande importanza in seguito.

Alla luce di questo teorema, risulta importante saper calcolare in modo efficiente i valori della funzione ϕ che, al momento, è definita in maniera un po' implicita.

Proposizione 14.24. *Se b e c sono due numeri primi tra loro*

$$\phi(bc) = \phi(b)\phi(c)$$

Dimostrazione. Facciamo una breve osservazione preliminare: dati tre numeri interi s, t, m, con $m > 0$, tali che $s \equiv t \pmod{m}$, allora s è coprimo con m se e solo se t è coprimo con m. Infatti $s \equiv t \pmod{m}$ può essere tradotto nella relazione $s = mq + t$ per un certo intero q, e dal Teorema 10.7 sappiamo che $MCD(s, m) = MCD(m, t)$.

Ora se u è un numero intero positivo coprimo con bc e minore di bc, allora u è in particolare coprimo con b e coprimo con c, ed è dunque soluzione di un sistema di equazioni del tipo:

$$\begin{cases} x \equiv k & (b) \\ x \equiv v & (c) \end{cases}$$

dove k è un intero positivo coprimo con b e $< b$ e v è un intero positivo coprimo con c e $< c$. Viceversa, per il teorema cinese, ogni sistema di equazioni del tipo descritto ha una sola soluzione intera positiva e $< bc$, e tale soluzione, essendo coprima con b e con c, è anche coprima con bc.

Dunque i numeri interi positivi coprimi con bc e minori di bc sono tanti quanti i sistemi del tipo descritto, che sono $\phi(b)\phi(c)$ (il prodotto delle possibile scelte di k e v).

□

Teorema 14.25. *Consideriamo un intero positivo m. Se $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ è la sua decomposizione in fattori primi, allora*

$$\phi(m) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_k^{a_k} - p_k^{a_k-1})$$

Dimostrazione. Dalla Proposizione 14.24 segue subito che per calcolare $\phi(m)$ basta fare il prodotto dei numeri $\phi(p_i^{a_i})$. Ci resta dunque da sapere quanto vale $\phi(p^n)$ con p numero primo. Osserviamo che i numeri positivi minori di p^n sono tutti primi con p^n a meno che non siano multipli di p. Un semplice calcolo mostra dunque che $\phi(p^n) = p^n - p^{n-1}$. □

Osservazione 14.26. In particolare, se p e q sono due distinti numeri primi, $\phi(p^2) = p^2 - p$, $\phi(pq) = (p-1)(q-1)$. Dunque, come avevamo osservato nell'Esempio 14.19, $\phi(10) = 4 \cdot 1 = 4$, $\phi(15) = 4 \cdot 2 = 8$.

Esempio 14.27. Come applicazione immediata dei risultati precedenti possiamo calcolare subito la classe di resto di 2^{365} modulo 225.

Visto che $\phi(225) = (25-5)(9-3) = 120$, per il Teorema 14.21 sappiamo infatti che

$$2^{120} \equiv 1 \bmod 225$$

Dunque

$$2^{365} \equiv (2^{120})^3 \cdot 2^5 \equiv 2^5 \equiv 32 \bmod 225$$

ESEMPIO 14.28. Il Teorema 14.21 ci dice che

$$2^8 \equiv 1 \bmod 15$$

Osserviamo però che l'ordine di $[2]$ in $\mathbb{Z}_{15}^*$ non è 8, ma 4. L'ordine di un elemento divide l'ordine del gruppo (Corollario 14.17): questo esempio mostra che non è detto che coincida con l'ordine del gruppo. Del resto, $[1]$ ha ordine 1 in ogni gruppo $\mathbb{Z}_m^*$, e, se $m > 1$, 1 è diverso da $\phi(m)$.

Trovate il Teorema di Lagrange e degli esercizi su congruenze con esponenziali a pag. 103 di [**?**].

4. Esercizi

ESERCIZIO 14.29. Dimostrare che se la cardinalità di un gruppo è un numero primo, allora il gruppo è ciclico.

ESERCIZIO 14.30. Dimostrare che se per due elementi a, b di un gruppo G vale $ab = e$ allora vale anche $ba = e$, e viceversa. Dunque per verificare che b è l'inverso di a basta verificare solo che sia inverso sinistro (o solo che sia inverso destro).

ESERCIZIO 14.31. Quali sono gli elementi di ordine massimo in $\mathbb{Z}_{13}^*$? E in $\mathbb{Z}_{20}^*$?

ESERCIZIO 14.32. Sia G un gruppo abeliano finito di cardinalità n. Dimostrare, senza usare il teorema di Lagrange, e imitando la prima dimostrazione del piccolo teorema di Fermat, che per ogni $g \in G$ vale $g^n = e$. [Nota: seguendo questa strada avremmo potuto dunque dimostrare il teorema di Eulero senza passare per il Teorema di Lagrange.]

ESERCIZIO 14.33. Se H è un sottoinsieme finito non vuoto di un gruppo G e vale che $a, b \in H \Rightarrow ab \in H$, allora H è un sottogruppo di G.

ESERCIZIO 14.34. Sia p un numero primo dispari. Dimostrare che se $[-1]$ è un quadrato in $\mathbb{Z}_p$ allora p è congruo a 1 modulo 4.

ESERCIZIO 14.35. Dimostrare che, preso un numero primo $p \equiv 1 \bmod 4$ allora

$$\left(\left(\frac{(p-1)}{2}\right)!\right)^2 \equiv -1 \bmod p$$

ESERCIZIO 14.36. Dimostrare che esistono infiniti numeri primi congrui a 1 modulo 4.

SOLUZIONE: [Traccia] Se fossero finiti, diciamo $p_1, p_2, \ldots, p_N$, potremmo considerare il numero $4(p_1 p_2 \cdots p_N)^2 + 1$... □

ESERCIZIO 14.37. Dato un sottogruppo H di un gruppo G si consideri la seguente relazione fra gli elementi di G: $x \sim y$ se e solo se $y^{-1}x \in H$.

Dimostrare che si tratta di una relazione di equivalenza e che per due elementi x e y vale $x \sim y$ se e solo se x e y appartengono allo stesso laterale destro $xH = yH$.

Esercizio 14.38. Dimostrare che, per ogni intero positivo n vale:

$$n = \sum_{d|n} \phi(d)$$

Esercizio 14.39. Sia $\mathcal{F}_n$ l'ennesimo numero di Fermat (vedi l'Esercizio 11.38)[3]. Dimostrare che, se q è un primo che divide $\mathcal{F}_n$, allora

$$q \equiv 1 \bmod 2^{n+1}$$

Esercizio 14.40 (Più difficile del precedente). Proviamo a migliorare il risultato dell'esercizio precedente, dimostrando la seguente osservazione[4]: se q è un primo che divide $\mathcal{F}_n$, con $n > 1$, allora

$$q \equiv 1 \bmod 2^{n+2}$$

[3]Il risultato di questo esercizio potrebbe fornire una spiegazione di come mai Eulero ha saputo trovare facilmente il numero primo 641 che divide $\mathcal{F}_5$: per cercare un eventuale primo che divide $\mathcal{F}_5$ basta cercare fra i numeri primi congrui a 1 modulo $2^6 = 64$ o, se dimostrate anche il risultato del prossimo esercizio, addirittura fra i numeri primi congrui a 1 modulo $2^7 = 128$. Chi cerca fra i numeri primi congrui a 1 modulo 128 trova come primo candidato il 257 e poi subito dopo, al secondo tentativo, il 641.

[4]Dovuta al matematico francese Edouard Lucas, 1842-1891.

CAPITOLO 15

Alcune osservazioni sulla fattorizzazione dei polinomi

1. Polinomi irriducibili e teorema di fattorizzazione unica

In questo paragrafo, che tratterà della fattorizzazione di polinomi, considereremo (per motivi che diverranno chiari nel corso del paragrafo stesso) anche polinomi a coefficienti in $\mathbb{Z}$, ovvero in un anello che non è un campo. Cercheremo di sottolineare le differenze principali nei due casi, una per esempio è che in $\mathbb{Z}[x]$ non è più vero che tutti i polinomi di grado 0 (ovvero le costanti non nulle) sono invertibili: gli unici polinomi invertibili sono il polinomio 1 e il polinomio -1 (per le altre costanti a non esiste un polinomio di grado 0 b in $\mathbb{Z}[x]$ tale che $a \cdot b = 1$). Useremo la notazione $A[x]$ quando considereremo il caso allargato di polinomi a coefficienti in un anello A commutativo, con unità e privo di divisori di zero.[1] I casi che ci interesseranno saranno essenzialmente quelli dei polinomi a coefficienti in $\mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, dunque tutti del tipo descritto e, a parte $\mathbb{Z}$, tutti campi.

Cominciamo introducendo il concetto di polinomio irriducibile in $A[x]$, che avrà lo stesso ruolo del concetto di numero primo in $\mathbb{Z}$.

Definizione 15.1. Dato un polinomio $p(x)$ di $A[x]$ con A anello, se esistono due polinomi $f(x)$ e $g(x)$ in $A[x]$ entrambi non invertibili e tali che

$$p(x) = f(x) \cdot g(x)$$

il prodotto $f(x) \cdot g(x)$ si dice **una fattorizzazione** di $p(x)$ in $A[x]$.

A questo punto possiamo caratterizzare quelli che vogliamo chiamare polinomi irriducibili in $A[x]$:

Definizione 15.2. Sia $f(x)$ un polinomio di $A[x]$ non invertibile. Il polinomio $f(x)$ si dice **riducibile** (o fattorizzabile) in $A[x]$ se in $A[x]$ esiste almeno una fattorizzazione di $f(x)$. Altrimenti il polinomio $f(x)$ si dice **irriducibile**.

Osservazione 15.3. Un modo equivalente di dire che un polinomio $f(x)$ di $A[x]$ è irriducibile (ed è quello che solitamente viene richiamato negli esercizi e nelle dimostrazioni) è affermare che qualsiasi scrittura di $f(x)$ come prodotto di polinomi di $A[x]$:

$$f(x) = g(x)h(x)$$

implica che uno dei due polinomi sia invertibile in $A[x]$. Ovvero nel caso di polinomi a coefficienti in un campo $\mathbb{K}$, essendo gli invertibili tutti e soli i polinomi di grado 0 (le costanti), $f(x)$ è irriducibile in $\mathbb{K}[x]$ se e solo se $f(x)$ ha grado maggiore o uguale a 1 e non può essere scritto come prodotto di due polinomi (non necessariamente distinti) di grado maggiore di 0.

Cominciamo a discutere qualche proprietà sulla irriducibilità che vale nei $\mathbb{K}[x]$ (ma in generale, vedremo, non vale per gli $A[x]$).

[1] Si dice in tal caso che A è un dominio. Per esempio l'anello Z è un dominio, mentre l'anello $\mathbb{Z}_{15}$ non lo è.

PROPOSIZIONE 15.4. *Negli anelli di polinomi $\mathbb{K}[x]$, con $\mathbb{K}$ campo, tutti i polinomi di grado 1 sono irriducibili.*

DIMOSTRAZIONE. Supponiamo che il polinomio $f(x) \in \mathbb{K}[x]$ di grado 1 sia il prodotto di due polinomi $g(x)$ e $h(x)$ di $\mathbb{K}[x]$:

$$f(x) = g(x)h(x)$$

Per le proprietà del grado del prodotto di polinomi abbiamo che:

$$1 = deg(f(x)) = deg(g(x)) + deg(h(x))$$

Ovvero uno dei due polinomi deve avere grado 0. E sappiamo che in $\mathbb{K}[x]$ tutti i polinomi di grado 0 sono invertibili. □

OSSERVAZIONE 15.5. Mostriamo, ad esempio, che in $\mathbb{Z}[x]$ esistono polinomi di primo grado riducibili. Consideriamo $f(x) = 2x - 4$, possiamo scriverlo come $2 \cdot (x - 2)$ ed i polinomi 2 e $x - 2$ non sono invertibili in $\mathbb{Z}[x]$.

DEFINIZIONE 15.6. Un polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$ in $\mathbb{Z}[x]$ si dice **primitivo** se il massimo comun divisore tra i suoi coefficienti $a_0, a_1, \ldots, a_n$ è uguale a 1.

La definizione di polinomio primitivo ci permette di individuare i polinomi irriducibili di primo grado in $\mathbb{Z}[x]$ (e dunque di mostrare che, per esempio, il polinomio $x - 2$ è irriducibile in $\mathbb{Z}[x]$).

PROPOSIZIONE 15.7. *In $\mathbb{Z}[x]$ i polinomi di primo grado sono irriducibili se e solo se sono primitivi.*

DIMOSTRAZIONE. Se $f(x) = ax + b \in \mathbb{Z}[x]$ di primo grado è il prodotto di due polinomi, allora, per la proprietà del grado[2], deve essere il prodotto di un polinomio di primo grado $h(x) = sx + t$, per un polinomio di grado 0, ovvero una costante $c \in \mathbb{Z}$. Questo, per la definizione di uguaglianza tra polinomi significa che $c \cdot s = a$ e $c \cdot t = b$, dunque che c è un divisore comune dei coefficienti di $f(x)$. Dunque esiste c non invertibile (ovvero diverso da 1 o -1), e quindi una fattorizzazione di $f(x)$ (ovvero $c \cdot h(x)$) se e solo se $f(x)$ non è primitivo. □

Abbiamo dunque discusso l'irriducibilità dei polinomi di grado 1 in $\mathbb{K}[x]$ e in $\mathbb{Z}[x]$. Per quanto riguarda i polinomi di grado maggiore di 1, una discussione importante è quella che lega la irriducibilità di un polinomio $f(x)$ in $\mathbb{K}[x]$ di grado $n > 1$ al fatto che esso abbia radici in $\mathbb{K}$. Dal teorema di Ruffini segue che se $f(x)$ ha una radice α in $\mathbb{K}$ allora è riducibile. Infatti si ha che il polinomio $(x - \alpha)$ divide $f(x)$:

$$\underbrace{f(x)}_{grado>1} = g(x) \cdot \underbrace{(x-1)}_{grado=1}$$

Inoltre, per le proprietà del grado, $g(x)$ ha grado maggiore di 0, ovvero non è invertibile.

Viceversa in generale **non è vero** che se un polinomio di grado maggiore di 1 non ha radici allora è irriducibile. Ad esempio il polinomio $x^4 + 2x^2 + 1$ di $\mathbb{R}[x]$ è riducibile in $\mathbb{R}[x]$:

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

ma non ha radici in $\mathbb{R}$ (non esiste nessun numero reale che elevato al quadrato è uguale a -1).

L'unica cosa certa è che un polinomio che non ha radici in $\mathbb{K}$ allora non ha fattori di grado 1 nella sua fattorizzazione in $\mathbb{K}[x]$. Da questo segue che:

[2]Le proprietà del grado continuano a valere in $A[x]$ con A dominio, come potete facilmente verificare.

COROLLARIO 15.8. *Un polinomio $f(x) \in \mathbb{K}[x]$ di grado 2 e 3 è riducibile se e solo se ha una radice in $\mathbb{K}$.*

DIMOSTRAZIONE. Abbiamo osservato che, in generale, un polinomio di grado $n > 1$ che ha una radice in $\mathbb{K}$ è riducibile in $\mathbb{K}[x]$. Viceversa se un polinomio di grado 2 o 3 è riducibile allora, sfruttando le proprietà del grado del prodotto di polinomi, necessariamente nel primo caso ($n = 2$) deve essere il prodotto di due fattori di grado 1, mentre nel secondo caso ($n = 3$) può essere il prodotto di un polinomio di grado 1 per un polinomio di grado 2 o il prodotto di tre polinomi di grado 1. Ovvero abbiamo stabilito che i polinomi di grado 2 o 3 riducibili hanno necessariamente un fattore di grado 1 e il teorema di Ruffini ci dice che avere un fattore di grado 1 in $\mathbb{K}[x]$ equivale ad avere una radice in $\mathbb{K}$. □

Gli elementi irriducibili di $\mathbb{K}[x]$ hanno molte analogie con i numeri primi di $\mathbb{Z}$. Un primo risultato importante è quello che ci dice che *se un polinomio irriducibile divide un prodotto di polinomi, allora divide uno dei due fattori.* Enunciamo questo risultato nel seguente teorema, la cui dimostrazione, lasciata come esercizio, coinvolge, analogamente a quello che accade in $\mathbb{Z}$, il lemma di Bezout.

TEOREMA 15.9 (Primalità di un polinomio irriducibile). *Se $p(x)$ è un polinomio irriducibile in $\mathbb{K}[x]$ dove $\mathbb{K}$ è un campo, e $p(x) \mid f(x) \cdot g(x)$ (dove $f(x), g(x) \in \mathbb{K}[x]$), allora o vale $p(x) \mid f(x)$ o vale $p(x) \mid g(x)$.*

Vale anche l'analogo del teorema di fattorizzazione unica (la dimostrazione è un esercizio caldamente consigliato; è una applicazione del teorema di primalità: si procede in maniera del tutto simile alla dimostrazione della fattorizzazione unica in $\mathbb{Z}$).

TEOREMA 15.10 (Teorema di fattorizzazione unica per polinomi). *Ogni polinomio di grado ≥ 1 in $\mathbb{K}[x]$ (dove $\mathbb{K}$ è un campo) è irriducibile o si fattorizza come prodotto di polinomi irriducibili. Inoltre, se*

$$f(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_s(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_t(x)$$

sono due fattorizzazioni del polinomio $f(x)$ come prodotto di irriducibili, allora vale che $s = t$ e che i polinomi $p_i(x)$ e i polinomi $q_j(x)$ sono a due a due associati.

Nel teorema di fattorizzazione unica per polinomi i $p_i(x)$ non sono necessariamente distinti. Proprio come nel caso della fattorizzazione tra gli interi, possiamo scrivere la fattorizzazione di un polinomio *accorpando* i fattori uguali e usando le potenze. Si scriverà dunque

$$h(x) = a \cdot q_1^{r_1}(x) \cdot q_2^{r_2}(x) \cdots q_t^{r_t}(x)$$

dove a è il coefficiente direttivo di $h(x)$, i $q_j(x)$ sono i polinomi irriducibili distinti monici[3] della fattorizzazione di $h(x)$, gli r_i sono i numeri naturali positivi che evidenziano quante volte ricorre il polinomio $q_i(x)$ nella fattorizzazione di $h(x)$.[4]

Avendo questa fattorizzazione è molto facile individuare, proprio come avveniva in $\mathbb{Z}$, il $M.C.D.$ di due polinomi (se non si conosce già una fattorizzazione, in generale è invece più conveniente. Se infatti consideriamo un polinomio $g(x)$ e la sua fattorizzazione in irriducibili:

$$g(x) = b \cdot p_1^{s_1}(x) p_2^{s_2}(x) \cdot \ldots \cdot p_j^{r_j}(x)$$

[3]Un polinomio monico è un polinomio in cui il coefficiente del termine di grado più alto è uguale a 1, tipo $f(x) = x^4 + 6x^3 + x + 6$ in $\mathbb{R}[x]$.

[4]Detto in formule r_i è quel numero naturale tale che $q_i(x)^{r_i}$ divide $h(x)$ e $q_i(x)^{r_i+1}$ non divide $h(x)$.

allora il *M.C.D.* $(h(x), g(x))$ si otterrà facendo il prodotto degli irriducibili che compaiono sia fra i $p_m(x)$ che fra i $q_n(x)$, ciascuno preso col minimo esponente fra i due esponenti che troviamo nelle due fattorizzazioni.

Esempio 15.11. Consideriamo in $\mathbb{Q}[x]$,

$$h(x) = (x-1)^2(x^2-5)^3(x^4-7x+7)$$

e

$$g(x) = (x-1)^7(x^2-5)(x^5+11x^2+11)^2$$

e supponiamo di sapere che i fattori che compaiono nelle fattorizzazioni sono irriducibili (presto discuteremo un criterio che permette di verificarlo facilmente); allora il *M.C.D.* $(h(x), g(x))$ è

$$(x-1)^2(x^2-5)$$

Gli altri *M.C.D.* $(h(x), g(x))$, come sappiamo, sono tutti i polinomi associati a $(x-1)^2(x^2-5)$.

Osservazione 15.12. L'unicità della fattorizzazione in $\mathbb{K}[x]$ è a meno dell'ordine dei fattori e di moltiplicazione per invertibili, cioè le costanti. Ovvero la fattorizzazione $(x-1)\cdot(x-2)$ del polinomio x^2-3x+2 potrebbe essere scritta anche $(x-2)\cdot(x-1)$, ma questa fattorizzazione la consideriamo identica alla precedente, abbiamo cambiato solo l'ordine dei fattori. Così come consideriamo identica la fattorizzazione $\frac{1}{2}\cdot(x-1)\cdot 2\cdot(x-2)$, in quanto abbiamo solo moltiplicato per invertibili (il cui prodotto è 1) i due fattori irriducibili.

Anche in questo caso osserviamo l'analogia con l'unicità della fattorizzazione in primi dei numeri in $\mathbb{Z}$. Il numero 21 è uguale a $7\cdot 3$; noi consideriamo identica (perchè cambiamo solo l'ordine) la fattorizzazione $3\cdot 7$, ma anche la fattorizzazione che si può ottenere moltiplicando per invertibili il cui prodotto totale sia 1. Gli invertibili in $\mathbb{Z}$ sono 1 e -1. Dunque 21 lo possiamo fattorizzare anche come $-1\cdot 3\cdot(-1)\cdot 7$ ovvero come $-3\cdot(-7)$.

Osservazione 15.13. Il teorema di fattorizzazione unica vale per ogni $\mathbb{K}[x]$ con $\mathbb{K}$ campo. Per la dimostrazione usiamo il teorema di primalità che a sua volta si dimostra tramite il teorema di Bezout che vale in $\mathbb{K}[x]$ con K campo. Cosa succede se l'insieme dei coefficienti A è un anello ma non un campo? Vale la fattorizzazione unica? La risposta è *"dipende"*... Si può infatti dimostrare che il teorema di fattorizzazione unica vale anche in $\mathbb{Z}[x]$, ma anche mostrare esempi di anelli (che non sono campi) per cui il il teorema di fattorizzazione unica non vale. Consideriamo ad esempio l'insieme $\mathbb{Z}_{30}[x]$ ed il polinomio x^2-1. Facendo i conti si può verificare che:

$$x^2-1 = (x-1)(x-29) = (x-19)(x-11)$$

Queste sono due distinte fattorizzazioni in irriducibili.

2. Fattorizzazione in $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$

Affrontiamo ora il problema della fattorizzazione nell'anello dei polinomi $\mathbb{K}[x]$, variando $\mathbb{K}$ tra uno dei seguenti campi: $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

2.1. Fattorizzazione in $\mathbb{C}[x]$. Il campo $\mathbb{C}$ dei numeri complessi ha una proprietà molto importante per quanto riguarda le radici di polinomi a coefficienti in $\mathbb{C}$, proprietà che non a caso si chiama **teorema fondamentale dell'algebra** e di cui noi riportiamo solo l'enunciato (la dimostrazione di questo risultato esula dagli obiettivi di questo testo).

TEOREMA 15.14 (Teorema fondamentale dell'algebra). *Ogni polinomio $f(x)$ a coefficienti in $\mathbb{C}$ di grado maggiore di zero ammette almeno una radice in $\mathbb{C}$.*

Usando il teorema fondamentale dell'algebra e il teorema di Ruffini abbiamo una caratterizzazione completa degli irriducibili in $\mathbb{C}$. Infatti una immediata conseguenza è che:

COROLLARIO 15.15. *Ogni polinomio $f \in \mathbb{C}[x]$ di grado $n > 0$ è il prodotto di n fattori di primo grado in $\mathbb{C}[x]$.*

DIMOSTRAZIONE. Procediamo per induzione sul grado n di f. Se f è di primo grado la tesi segue immediatamente. Sia ora $f(x) = \sum_{i=0}^{n} a_i x^i$ con $a_i \in \mathbb{C}$ e $a_n \neq 0$, $n > 1$. Possiamo scrivere $f(x) = a_n g(x)$ con $g(x)$ monico. Sia α radice di $g(x)$, la cui esistenza è assicurata dal Teorema 15.14 allora:

$$f(x) = a_n(x - \alpha)g_1(x) \quad \text{con} \quad deg(g_1) = n - 1$$

quindi g_1 e di conseguenza f si scrivono come prodotto di fattori di grado 1. □

Dal Corollario 15.15 segue che:

In $\mathbb{C}[x]$ un polinomio è irriducibile se e solo se è di primo grado

In $\mathbb{C}[x]$ quindi fattorizzare un polinomio equivale a trovarne le radici perchè tutti i suoi fattori irriducibili sono di grado 1. Dobbiamo cioè essere in grado di risolvere equazioni polinomiali a coefficienti complessi, cosa che può essere anche molto complicata. Prima di vedere un esempio, sottolineiamo il fatto che la ricerca di radici complesse è importante, come vedremo, anche per la fattorizzazione in $\mathbb{R}[x]$.

ESEMPIO 15.16. Fattorizzare il polinomio $x^2 + 4x + 5 \in \mathbb{C}[x]$ come prodotto di irriducibili.

Dobbiamo trovare le radici complesse del polinomio $x^2 + 4x + 5$, ovvero le soluzioni complesse dell'equazione

$$x^2 + 4x + 5 = 0 \tag{15.1}$$

La formula risolutiva dell'equazione di secondo grado ci permette di trovare le soluzioni complesse (anche se il delta è negativo!):

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Nel nostro caso:

$$x_{1,2} = \frac{-4 \pm 2i}{2} = -2 \pm i$$

Quindi il polinomio $x^2 + 4x + 5 \in \mathbb{C}[x]$ si fattorizza in irriducibili come:

$$(x - (-2 + i)) \cdot (x - (-2 - i))$$

Per riprova possiamo calcolarci questo prodotto osservando che:

$$(x - (-2 + i)) \cdot (x - (-2 - i)) = ((x + 2) + i) \cdot ((x + 2) - i)$$

E questo sappiamo essere un prodotto notevole (ovvero la differenza di quadrati):

$$((x + 2) + i) \cdot ((x + 2) - i) = (x + 2)^2 - i^2 = x^2 + 4x + 5$$

Per la ricerca di radici complesse in polinomi a coefficienti reali (e dunque utile sia per la fattorizzazione in $\mathbb{C}[x]$ che in $\mathbb{R}[x]$) è importante ricordare la funzione coniugio da $\mathbb{C}$ in $\mathbb{C}$:

DEFINIZIONE 15.17. Chiamiamo funzione **coniugio** la funzione da $\mathbb{C}$ in $\mathbb{C}$ che al numero complesso $a+ib$ associa $\overline{a+ib}=a-ib$.

ESERCIZIO 15.18. Usando la definizione dimostrare le seguenti proprietà della funzione coniugio:

(1) I suoi punti fissi, ovvero gli $z\in\mathbb{C}$ tali che $\overline{z}=z$, sono tutti e soli i numeri reali.
(2) Il coniugio della somma è la somma dei coniugi, ovvero per ogni $z,w\in\mathbb{C}$ $\overline{z+w}=\overline{z}+\overline{w}$.
(3) Il coniugio del prodotto è il prodotto dei coniugi, ovvero per ogni $z,w\in\mathbb{C}$ $\overline{z\cdot w}=\overline{z}\cdot\overline{w}$.
(4) Il prodotto di un numero complesso per il suo coniugato è un numero reale, ovvero per ogni $z\in\mathbb{C}$ si ha che $z\cdot\overline{z}\in\mathbb{R}$.

Il coniugio permette di dimostrare una interessante proprietà delle radici complesse di un polinomio a coefficienti reali (**ATTENZIONE:** sottolineiamo il fatto che tra le ipotesi che stiamo considerando c'è che i coefficienti del polinomio siano reali), ovvero che se z è una radice di un polinomio $p(x)$ a coefficienti reali, allora $\overline{z}$ è una radice di $p(x)$. Questo è ovvio, ma non è di nessuna utilità, se z è reale in quanto $\overline{z}=z$, ma è invece importante nel caso in cui $z\in\mathbb{C}-\mathbb{R}$:

PROPOSIZIONE 15.19. *Sia $f(x)\in\mathbb{R}[x]\subset\mathbb{C}[x]$ e sia $\alpha\in\mathbb{C}$ una radice di f. Allora anche $\overline{\alpha}$ è una radice di f.*

DIMOSTRAZIONE. sia $f(x)=\sum_{i=0}^{n}a_ix^i$ con $a_i\in\mathbb{R}$. Per ipotesi:

$$0=f(\alpha)=\sum_{i=0}^{n}a_i\alpha^i$$

quindi, dall'enunciato dell'Esercizio 15.18, segue che:

$$\overline{0}=\overline{\sum_{i=0}^{n}a_i\alpha^i}=\sum_{i=0}^{n}\overline{a_i\alpha^i}=\sum_{i=0}^{n}a_i\overline{\alpha^i}=\sum_{i=0}^{n}a_i\overline{\alpha}^i$$

Cioè $f(\overline{\alpha})=\overline{0}=0$. □

Nel prossimo esercizio useremo il risultato della Proposizione 15.19 per fattorizzare un polinomio a coefficienti reali in $\mathbb{C}[x]$.

ESERCIZIO 15.20. Sapendo che $f(x)=x^4-4x^3+3x^2+14x+26$ ha radice $3+2i$, fattorizzare il polinomio in $\mathbb{C}[x]$.

Risoluzione. Il polinomio considerato è a coefficienti interi, quindi in particolare reali. Allora possiamo applicare la Proposizione 15.19 e concludere che anche $3-2i$ è radice del polinomio; da questo segue che $(x-(3+2i))\cdot(x-(3-2i))=x^2-6x+13$ divide $f(x)$:

$$\begin{array}{rrrrr|l}
x^4 & -4x^3 & +3x^2 & +14x & +26 & x^2-6x+13\\
x^4 & -6x^3 & +13x^2 & & & x^2+2x+2\\
\cline{1-5}
 & 2x^3 & -10x^2 & +14x & +26 & \\
 & 2x^3 & -12x^2 & +26x & & \\
\cline{1-5}
 & & 2x^2 & -12x & +26 & \\
 & & 2x^2 & -12x & +26 & \\
\cline{1-5}
 & & & & 0 &
\end{array}$$

Quindi:

$$f(x) = \underbrace{(x-(3+2i))\cdot(x-(3-2i))}_{x^2-6x+13}\cdot(x^2+2x+2)$$

E per completare la fattorizzazione in $\mathbb{C}[x]$ resta da fattorizzare il polinomio x^2+2x+2. Calcoliamo le radici del polinomio attraverso la formula risolutiva delle equazioni di secondo grado:

$$x_{1,2} = \frac{-2\pm\sqrt{-4}}{2} = \frac{-2\pm 2i}{2} = \frac{2\cdot(-1\pm i)}{2} = -1\pm i$$

Per cui la fattorizzazione di $f(x)$ è data da:

$$(x-(3+2i))\cdot(x-(3-2i))\cdot(x+(1+i))\cdot(x+(1-i))$$

Osservazione 15.21. Osserviamo, senza ancora aver parlato di fattorizzazione in $\mathbb{R}[x]$, che la fattorizzazione in $\mathbb{C}[x]$ del polinomio $f(x) = x^4-4x^3+3x^2+14x+26$ dell'Esercizio 15.20 fornisce indicazioni importanti sulla fattorizzazione dello stesso polinomio in $\mathbb{R}[x]$.

2.2. Fattorizzazione in $\mathbb{R}[x]$. Anche in $\mathbb{R}[x]$ si possono caratterizzare i polinomi irriducibili attraverso il grado, utilizzando quello che sappiamo della fattorizzazione in $\mathbb{C}[x]$.

Consideriamo un generico polinomio $f(x)\in\mathbb{R}[x]$ di grado n. In particolare $f(x)$ può essere visto come elemento di $\mathbb{C}[x]$ e indichiamo con $z_1,\dots,z_r$ le sue radici complesse e con $m_1,\dots,m_r$ le loro rispettive molteplicità[5]. La fattorizzazione di $f(x)$ in $\mathbb{C}[x]$ è dunque la seguente:

$$\prod_{i=1}^{r}(x-z_i)^{m_i} \tag{15.2}$$

Come si passa dalla fattorizzazione in $\mathbb{C}[x]$ a quella in $\mathbb{R}[x]$? Si osserva che se $z_i\in\mathbb{R}$ allora $(x-z_i)^{m_i}$ è un fattore di $f(x)$ in $\mathbb{R}[x]$, mentre se $z_i\in\mathbb{C}-\mathbb{R}$, allora il fattore $(x-z_i)^{m_i}$ non appartiene a $\mathbb{R}[x]$, ma sappiamo che esiste un'altra radice z_j di $f(x)$ tale che $z_j=\overline{z_i}$ e $m_i=m_j$.
Dunque, nella fattorizzazione 15.2, è presente il fattore

$$((x-z_i)\cdot(x-\overline{z_i}))^{m_i}$$

L'osservazione chiave è che il fattore di secondo grado $(x-z_i)\cdot(x-\overline{z_i})$ è un polinomio reale. Infatti sia $z=a+ib$, $a,b\in\mathbb{R}$ e $b\neq 0$, allora:

$$(x-(\underbrace{a+ib}_{z}))\cdot(x-(\underbrace{a-ib}_{\overline{z}})) = x^2-2ax+a^2+b^2$$

Come anticipato, i coefficienti del polinomio (1, $-2a$ e a^2+b^2) sono reali.
Riassumendo, date le radici complesse $z_1,\dots,z_r$ di $f(x)$, se z_i è un numero reale allora $x-z_i$ è un fattore irriducibile di primo grado di $f(x)$ (ripetuto m_i volte) della fattorizzazione in $\mathbb{R}[x]$, se z_i non è un numero reale (ovvero $z_i=a+ib$ con $b\neq 0$) allora $(x-z_i)\cdot(x-\overline{z_i})$ è un fattore di secondo grado della fattorizzazione in $\mathbb{R}[x]$ (ripetuto m_i volte) ed è irriducibile. Quest'ultima proprietà deriva dal fatto che, essendo di secondo grado, o è irriducibile o è il prodotto di due fattori di primo grado. Ma questa seconda opzione possiamo escluderla in quanto, dal teorema di Ruffini sappiamo che i fattori di

[5]Sappiamo, dal Corollario 15.15, che $\sum_{i=1}^{r} m_i = n$, ma in generale $r\leq n$. È $r=n$ solo se $f(x)$ ha tutte radici distinte in $\mathbb{C}[x]$.

primo grado sono associati ad una radice nel campo, e sappiamo, per ipotesi, che le radici del polinomio (che sono z e $\overline{z}$) non sono reali ($b \neq 0$).[6].
Dunque la fattorizzazione 15.2 di $f(x)$ in $\mathbb{C}[x]$ fatta di tutti fattori di grado 1, si *trasforma* in una fattorizzazione in $\mathbb{R}[x]$ di $f(x)$ tenendo inalterati i fattori con radici reali e *accorpando* in fattori irriducibili di secondo grado quelli corrispondenti a radici non reali (moltiplicando $x - z$ per $x - \overline{z}$).
Abbiamo scoperto che:

PROPOSIZIONE 15.22. *Ogni polinomio di grado maggiore di* 2 *in* $\mathbb{R}[x]$ *è riducibile.*

DIMOSTRAZIONE. Infatti in $\mathbb{C}[x]$ il polinomio $f(x)$ ha $n = deg(f(x))$ radici (non necessariamente distinte)[7] $z_1, \ldots, z_n$. Se una di queste n radici è reale, allora $f(x)$ ha un fattore di grado 1 e dunque è riducibile, altrimenti se sono tutte radici complesse non reali, $f(x)$ è divisibile per il polinomio reale di secondo grado $(x - z_1) \cdot (x - \overline{z_1})$:

$$f(x) = (x - z_1) \cdot (x - \overline{z_1}) \cdot h(x)$$

E per la proprietà del grado del prodotto di polinomi, $h(x)$ ha grado maggiore di 1 e dunque non è invertibile. □

Per concludere la piena caratterizzazione degli irriducibili in $\mathbb{R}[x]$, sapendo che (Proposizione 15.4) in ogni campo i polinomi di grado 1 sono irriducibili, ci resta da approfondire il caso dei polinomi di grado 2. Ma questo è molto semplice, infatti dal Corollario 15.8, sappiamo che $f(x) \in \mathbb{K}[x]$ di grado 2 è riducibile se e solo se ha una radice in $\mathbb{K}$. Nel caso di $\mathbb{K} = \mathbb{R}$ è noto dalla scuola superiore che, se $f(x) = ax^2 + bx + c$ è un generico polinomio reale di grado 2, allora $f(x)$ ha radici in $\mathbb{R}$ se e solo se:

$$b^2 - 4ac \geq 0$$

Abbiamo dunque la completa caratterizzazione degli irriducibili in $\mathbb{R}[x]$:
In $\mathbb{R}[x]$ un polinomio è irriducibile se e solo è di primo grado oppure di secondo grado (del tipo $ax^2 + bx + c$ con $a \neq 0$) con $\Delta = b^2 - 4ac$ minore di zero.
Abbiamo dunque un *algoritmo* molto rapido per sapere se un polinomio $f(x)$ è riducibile in $\mathbb{R}[x]$ (basta guardare il grado ed eventualmente calcolare il delta nel caso il grado sia 2). Ma sapere che un polinomio $f(x)$ è riducibile non implica che la sua fattorizzazione in fattori irriducibili sia semplice da trovare.

ESERCIZIO 15.23. Fattorizzare il polinomio $x^4 - 2x^2 - 3 \in \mathbb{R}[x]$.

Questo polinomio è di grado 4 ed è dunque riducibile in $\mathbb{R}[x]$: o è il prodotto di quattro polinomi di grado 1 (4 radici reali non necessariamente distinte), o il prodotto di un polinomio di grado 2 e due di grado 1 (2 radici reali non necessariamente distinte e 2 complesse coniugate) o il prodotto di due polinomi di grado 2 (4 radici complesse a due a due coniugate e non necessariamente distinte). Come si evince da questa prima analisi sarebbe fondamentale riuscire a determinarne le radici complesse. Esiste una formula risolutiva per le equazioni di quarto grado, ma non la conosciamo e dunque cerchiamo di agire diversamente, osservando che il polinomio considerato è, in un certo senso, *particolare*: non ha termini di grado dispari. Possiamo quindi, con la semplice sostituzione $x^2 = t$, ottenere un polinomio di grado 2 associato a quello di partenza:

[6]Si poteva anche esprimere questa osservazione utilizzando il Corollario 15.8: un polinomio di grado 2 è irriducibile se e solo se non ha radici nel campo.

[7]Potrebbe essere anche tutte uguali e dunque una radice di molteplicità n.

$t^2 - 2t - 3$. Cerchiamo di fattorizzare questo polinomio in $\mathbb{R}[t]$. Dalla formula risolutiva delle equazioni di secondo grado otteniamo:

$$t_{1,2} = \frac{2 \pm \sqrt{16}}{2}$$

Ovvero $t^2 - 2t - 3 = (t-3) \cdot (t+1)$. Quindi:

$$x^4 - 2x^2 - 3 \underbrace{=}_{x^2=t} t^2 - 2t - 3 = (t-3) \cdot (t+1) \underbrace{=}_{t=x^2} (x^2-3) \cdot (x^2+1)$$

In questo caso è facile vedere che $x^2 + 1$ è irriducibile in $\mathbb{R}[x]$ (ha radici complesse i e $-i$), mentre $x^2 - 3 = (x - \sqrt{3}) \cdot (x + \sqrt{3})$. Concludendo si ha che la fattorizzazione in irriducibili di $x^4 - 2x^2 - 3 \in \mathbb{R}[x]$ è data da:

$$(x - \sqrt{3}) \cdot (x + \sqrt{3}) \cdot (x^2 + 1)$$

2.3. Fattorizzazione in $\mathbb{Q}[x]$. In $\mathbb{Q}[x]$, a differenza di quanto visto per $\mathbb{C}[x]$ e $\mathbb{R}[x]$, vedremo che per ogni naturale n esistono polinomi di grado n irriducibili.

Una prima osservazione importante viene offerta dal Lemma di Gauss enunciato (senza dimostrazione) qui sotto: nel caso di un polinomio primitivo a coefficienti interi, la sua irriducibilità in $\mathbb{Q}[x]$ è equivalente alla sua irriducibilità in $\mathbb{Z}[x]$. Questo è un risultato per niente banale e scontato: infatti, per esempio, se è vero che è ovvio che un polinomio $f(x) \in \mathbb{K}[x]$, riducibile in $\mathbb{K}[x]$, è riducibile in qualsiasi campo $\mathbb{L}$ che contenga strettamente $\mathbb{K}$ (basta considerare la stessa fattorizzazione, infatti i polinomi di $\mathbb{K}[x]$ sono in particolare polinomi di $\mathbb{L}[x]$), il viceversa non è in generale vero. Ad esempio qualsiasi polinomio di secondo grado irriducibile in $\mathbb{R}[x]$ (ad esempio $x^2 + 1$) è riducibile in $\mathbb{C}[x]$ (nel caso di $x^2 + 1$ è uguale a $(x - i) \cdot (x + i)$).

LEMMA 15.24 (Lemma di Gauss). *Sia $f(x) \in \mathbb{Z}[x]$. Se $f(x) = a(x)b(x)$ in $\mathbb{Q}[x]$ allora possiamo trovare due polinomi $a_1(x) \in \mathbb{Z}[x]$, associato a $a(x)$, e $b_1 \in \mathbb{Z}[x]$, associato a $b(x)$, tali che*

$$f(x) = a_1(x)b_1(x)$$

Riassumendo, $g(x) \in \mathbb{Q}[x]$ è riducibile se e solo se il polinomio primitivo a coefficienti interi $f(x)$ ad esso associato è riducibile in $\mathbb{Z}[x]$. Abbiamo in definitiva ridotto la fattorizzazione in $\mathbb{Q}[x]$ a quella in $\mathbb{Z}[x]$ con notevoli vantaggi come vedremo da qui in avanti.

Cominciamo mostrando un primo criterio molto utile per riconoscere (e costruire) polinomi irriducibili in $\mathbb{Q}[x]$.

TEOREMA 15.25 (Criterio di Eisenstein). *Sia*

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

un polinomio primitivo di grado maggiore di 1 a coefficienti interi. Se esiste un numero primo p tale che:

1. *p NON divide il coefficiente direttivo a_n,*
2. *p divide tutti gli a_i con $i < n$,*
3. *p^2 non divide il termine noto a_0,*

allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$, e dunque - per il lemma di Gauss - in $\mathbb{Q}[x]$.

DIMOSTRAZIONE. Supponiamo che $f(x)$ sia uguale al prodotto dei due polinomi $g(x) = \sum_{i=0}^{r} b_i x^i$ e $h(x) = \sum_{i=0}^{s} c_i x^i$ di $\mathbb{Z}[x]$, entrambi di grado maggiore o uguale a 1. Da $f(x) = g(x)h(x)$ e dalla definizione di uguaglianza tra polinomi, segue che tutti i

coefficienti del polinomio a destra sono uguali a tutti i coefficienti del polinomio a sinistra. Facendo i conti, otteniamo un sistema dove gli $n+1$ coefficienti a_i di $f(x)$ sono espressi tramite i coefficienti di $g(x)$ e $h(x)$ come segue[8]:

$$a_i = \sum_{j=0}^{i} b_j \cdot c_{i-j} \tag{15.3}$$

Partiamo *dal basso* del sistema 15.3: $a_0 = b_0 c_0$. Per ipotesi p divide a_0, ma p^2 non divide a_0: questo significa che p divide uno tra b_0 e c_0, ma non entrambi. Il ruolo dei b_i e dei c_i è simmetrico quindi possiamo, senza perdere di generalità, supporre che p divida b_0 e non c_0.

A questo punto la seconda equazione del sistema 15.3 è $a_1 = b_1 c_0 + b_0 c_1$, che diventa:

$$b_1 c_0 = a_1 - b_0 c_1$$

Ora sappiamo che p divide a_1 (ipotesi), p divide b_0 (appena stabilito) e dunque p divide $b_1 c_0$. Sappiamo anche che p non divide c_0 e di conseguenza divide b_1.

Iterando questo procedimento si ottiene che p divide ogni b_i e di conseguenza divide $a_n = b_r c_s$: ma questo è contro l'ipotesi. L'assurdo nasce dal fatto di aver supposto che $f(x)$, che verifica le tre condizioni del criterio di Eisenstein, possa essere scritto come prodotto di due polinomi di grado maggiore o uguale a 1. □

Come detto il criterio di Eisenstein permette di costruire polinomi irriducibili in $\mathbb{Q}[x]$ e addirittura permette di trovarne *infiniti* per ogni grado $n > 0$:

COROLLARIO 15.26. *In $\mathbb{Q}[x]$ esistono polinomi irriducibili di grado $n > 0$ qualsiasi.*

DIMOSTRAZIONE. Basta considerare il polinomio $x^n - 2$ ed applicare Eisenstein con primo $p = 2$. Infatti 2 divide il termine noto (2), ma il quadrato di p (4) non divide il termine noto. E infine 2 non divide il coefficiente direttivo (1). Lo stesso ragionamento permette di dimostrare che $x^n - p$, per un qualsiasi primo p, è irriducibile. □

Un altro punto importante per fattorizzare in $\mathbb{Q}[x]$ un polinomio $f(x)$ a coefficienti interi è il fatto che la conoscenza del coefficiente direttivo e del termine noto di $f(x)$ permette di limitare la ricerca delle *possibili* radici razionali di $f(x)$ (e dunque, in termini di fattorizzabilità, dei possibili fattori di grado 1 di $f(x)$) ad un insieme finito di numeri razionali. Per la precisione:

PROPOSIZIONE 15.27. *Se $f(x) \in \mathbb{Z}[x]$ e r/s (ridotto ai minimi termini, ovvero con $(r, s) = 1$) è una radice in $\mathbb{Q}$, allora r divide il termine noto e s divide il coefficiente direttivo di $f(x)$.*

DIMOSTRAZIONE. Sia $f(x) = \sum_{j=0}^{m} b_j x^j$ a coefficienti interi, l'ipotesi che r/s sia radice equivale a:

$$\sum_{i=0}^{n} b_i \left(\frac{r}{s}\right)^i = 0$$

Moltiplicando tutto per s^n si ottiene:

$$b_n r^n + \underbrace{b_{n-1} r^{n-1} s + \ldots + b_0 s^n}_{\text{è un multiplo di } s} = 0 \tag{15.4}$$

[8]Esclusivamente per semplicità di notazione consideriamo anche i coefficienti nulli di $g(x)$ e $h(x)$ dei termini di grado maggiore rispettivamente di r e s. Ovvero $b_j = 0$ se $j > r$ e $c_t = 0$ se $t > s$.

Per cui $s|b_n r^n$, ma essendo $(s,r)=1$ questo implica $s|b_n$. Analogamente se raccogliamo in 15.4 r, otteniamo che r deve dividere $b_0 s^n$, ma essendo $(r,s)=1$ questo implica che $r|b_0$. □

ESEMPIO 15.28. Consideriamo il polinomio $f(x) = x^4 + 3x^3 + x^2 - 6x - 6$. Dalla Proposizione 15.27 segue che se r/s è una radice razionale, allora r divide -6 e s divide 1. Ovvero sappiamo che le uniche radici razionali possibili di $f(x)$ sono da ricercare nell'insieme finito:

$$A = \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

Sostituendo in $f(x)$ non si trova 0 in nessuno di questi casi, dunque $f(x)$ non ha radici razionali.
ATTENZIONE: questo non significa che $f(x)$ sia irriducibile! Sappiamo solo che $f(x)$ non ha fattori di grado 1, ma potrebbe essere il prodotto di due fattori irriducibili di grado 2.

ESERCIZIO 15.1. Il polinomio dell'esempio precedente è irriducibile in $\mathbb{Q}[x]$?
Suggerimento: se non vi riesce leggete più avanti...

La Proposizione 15.27 è di fondamentale importanza in quanto limita ad un insieme finito e ristretto la ricerca di possibili radici razionali (e quindi fattori irriducibili di grado 1) di un polinomio a coefficienti interi. Questo permette per esempio di avere un algoritmo per discutere l'irriducibilità di polinomi di grado 2 e 3 in $\mathbb{Q}[x]$, infatti un polinomio di questo tipo o è irriducibile o ha una radice razionale.

ESERCIZIO 15.29. Dire se $f(x) = x^3 - x^2 - 8x + 12$ è irriducibile in $\mathbb{Q}[x]$.

Risoluzione. I divisori del termine noto sono $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$, i divisori del coefficiente del termine di grado massimo sono $\{\pm 1\}$ quindi le possibili radici razionali sono: $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$. Proviamo a calcolare la funzione polinomiale $f(x)$ per questi valori fino a che non troviamo una radice; se non la troviamo vuol dire che $f(x)$ è irriducibile in $\mathbb{Q}[x]$:

$$f(1) = 4 \neq 0 \quad f(-1) = 18 \neq 0 \quad f(2) = 0$$

Dunque $f(x)$ è riducibile e ha $(x-2)$ come fattore di grado 1.

A questo punto si potrebbe continuare a cercare altre radici razionali per vedere se ci sono altri fattori di $f(x)$ di grado 1 diversi da $(x-2)$, ma forse nel caso di un polinomio di grado 3 conviene procedere dividendo $f(x)$ per $(x-2)$ in modo da trovare un fattore di grado 2 che sappiamo dire se è riducibile o meno in $\mathbb{Q}[x]$ attraverso la formula risolutiva delle equazioni di secondo grado:

$$\begin{array}{rrrrl}
x^3 & -x^2 & -8x & +12 & \mid\ x-2 \\
x^3 & -2x^2 & & & \mid\ x^2+x-6 \\
 & x^2 & -8x & +12 & \mid \\
 & x^2 & -2x & & \mid \\
 & & -6x & +12 & \mid \\
 & & -6x & +12 & \mid \\
 & & & 0 & \mid
\end{array}$$

Quindi $f(x) = (x-2)\cdot(x^2+x-6)$. Si tratta di vedere se $x^2+x-6=0$ ha o meno due soluzioni razionali. Dalla formula risolutiva si ottiene:

$$x_{1,2} = \frac{-1 \pm \sqrt{25}}{2} = \frac{-1 \pm 5}{2}$$

E quindi x^2+x-6 è riducibile in $\mathbb{Q}[x]$ e si fattorizza come $(x+3)\cdot(x-2)$. La fattorizzazione in irriducibili di $x^3 - x^2 - 8x + 12$ in $\mathbb{Q}[x]$ è dunque data da:

$$x^3 - x^2 - 8x + 12 = (x - 2)^2 \cdot (x + 3)$$

A questo punto cominciamo ad avere diversi strumenti per la fattorizzazione in $\mathbb{Q}[x]$: innanzitutto sappiamo che ci possiamo ridurre ad un polinomio, associato a quello di partenza, primitivo e a coefficienti interi. Sui polinomi primitivi a coefficienti interi conosciamo un criterio *diretto* di irriducibilità (Eisenstein). Inoltre, la fattorizzazione è molto più semplice in $\mathbb{Z}[x]$. Cerchiamo di capire perché riprendendo in mano il polinomio $f(x)$ dell'Esempio 15.28. Abbiamo già visto che non ha radici, dunque se è fattorizzabile è il prodotto di due polinomi di grado 2 (che per il lemma di Gauss possiamo supporre a coefficienti interi).

Consideriamo due generici polinomi di grado 2 in $\mathbb{Z}[x]$:

$$g(x) = ax^2 + bx + c$$
$$h(x) = dx^2 + ex + f$$

Per quanto osservato sopra, $f(x) = x^4 + 3x^3 + x^2 - 6x - 6$ è fattorizzabile se e solo se è il prodotto di due polinomi di grado 2, ovvero se e solo se esiste una soluzione del seguente sistema di 5 equazioni a coefficienti interi:

$$\begin{cases} 1 = a \cdot d \\ 3 = a \cdot e + b \cdot d \\ 1 = a \cdot f + b \cdot e + c \cdot d \\ -6 = b \cdot f + c \cdot e \\ -6 = c \cdot f \end{cases}$$

Sapere che, pur cercando la fattorizzazione in $\mathbb{Q}[x]$, possiamo risolvere in $\mathbb{Z}$ è di grande aiuto. Infatti risolvere *algoritmicamente* questo sistema in $\mathbb{Z}$ è possibile: ogni singola equazione infatti può avere solo un numero finito (anche uguale a 0) di soluzioni intere; studiando tutti i casi possibili e *risalendo* il sistema o si determina una soluzione intera o altrimenti si deduce che il sistema è irrisolvibile e dunque $f(x)$ è irriducibile in $\mathbb{Z}[x]$ e di conseguenza in $\mathbb{Q}[x]$. Questo procedimento di fattorizzazione in $\mathbb{Z}[x]$ risolvendo il sistema per casi è noto come **metodo della forza *bruta***. Applichiamo questo metodo al nostro sistema: vedremo così concretamente i vantaggi di sapere di potersi limitare a cercare soluzioni intere del sistema. Da $1 = a \cdot d$ ad esempio, segue che o $a = d = 1$ oppure $a = d = -1$ (ma se $f(x) = g(x) \cdot h(x)$, allora $f(x) = -g(x) \cdot (-h(x))$ e dunque possiamo considerare $a = d = 1$). Andiamo dunque a riscriverci il nostro sistema:

$$\begin{cases} 1 = a \cdot d \\ 3 = a \cdot e + b \cdot d \\ 1 = a \cdot f + b \cdot e + c \cdot d \\ -6 = b \cdot f + c \cdot e \\ -6 = c \cdot f \end{cases} \leftrightarrow \begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = f + b \cdot e + c \\ -6 = b \cdot f + c \cdot e \\ -6 = c \cdot f \end{cases}$$

Da $-6 = c \cdot f$ si ottiene che o $c = 1$ e $f = -6$, o $c = -1$ e $f = 6$, o $c = 2$ e $f = -3$ o infine $c = -2$ e $f = 3$ (essendo $g(x)$ e $h(x)$ dello stesso grado generici, il loro ruolo è completamente simmetrico e dunque non è necessario considerare anche i casi speculari tipo $c = 6$ e $f = -1$). Otteniamo dunque 4 sistemi con meno variabili. Bisogna studiarli

tutti:

$$\begin{cases} a=d=1 \\ 3=e+b \\ 1=-6+b\cdot e+1 \\ -6=-6b+e \\ c=1 \\ f=-6 \end{cases} \qquad \begin{cases} a=d=1 \\ 3=e+b \\ 1=6+b\cdot e-1 \\ -6=6b-e \\ c=-1 \\ f=6 \end{cases}$$

$$\begin{cases} a=d=1 \\ 3=e+b \\ 1=-3+b\cdot e+2 \\ -6=-3b+2e \\ c=2 \\ f=-3 \end{cases} \qquad \begin{cases} a=d=1 \\ 3=e+b \\ 1=3+b\cdot e-2 \\ -6=3b-2e \\ c=-2 \\ f=3 \end{cases}$$

È facile verificare che i primi tre sistemi non hanno soluzioni intere (portano rispettivamente alle seguenti equazioni irrisolvibili in $\mathbb{Z}$: $5e=12$, $7b=-3$, $5e=3$), mentre l'ultimo ha soluzione (con $b=0$ ed $e=3$). Dunque esiste una fattorizzazione di $f(x)$ in $\mathbb{Q}[x]$ (nonostante $f(x)$ non abbia radici razionali):

$$\underbrace{x^4+3x^3+x^2-6x-6}_{f(x)}=(\underbrace{x^2-2}_{g(x)})(\underbrace{x^2+3x+3}_{h(x)})$$

3. Esercizi

Esercizio 15.30. Sia $g(x)\in\mathbb{R}[x]$ il polinomio

$$g(x)=x^3-2x^2+2x-1$$

(1) Fattorizzare $g(x)$ in prodotto di polinomi irriducibili.
(2) Considerato il polinomio

$$f_a(x)=x^4-2ax^2+2ax-1$$

dimostrare che, per ogni $a\in\mathbb{R}$, un M.C.D. tra $g(x)$ e $f_a(x)$ è il polinomio $x-1$.

Risoluzione. Sappiamo che il polinomio $g(x)$ è riducibile in $\mathbb{R}[x]$, in quanto ha grado 3. Questo in particolare significa che $g(x)$ ha una radice reale. Osserviamo che non abbiamo studiato formule risolutive delle equazioni di terzo grado, quindi con i nostri strumenti possiamo trovare questa radice solo se è razionale (il polinomio che stiamo considerando in $\mathbb{R}[x]$ è a coefficienti interi): possiamo cioè provare tutte le possibili radici razionali che otteniamo dai divisori del coefficiente direttivo e del termine noto.
Però leggendo il testo dell'esercizio non abbiamo bisogno nemmeno di questo passaggio, infatti se dobbiamo mostrare che $x-1$ è un M.C.D. di $g(x)$ con un altro polinomio, allora $x-1$ dovrà essere un divisore di $g(x)$ (e quindi 1 una radice di $g(x)$). Andiamo a verificare che $x-1$ è un fattore irriducibile di $g(x)$: che sia irriducibile è certo, visto che è di grado 1; dobbiamo mostrare che effettivamente è un divisore di $g(x)$ (se così non fosse potremmo intanto concludere che l'affermazione della seconda parte dell'esercizio è falsa). In realtà si vede subito che $x-1$ è un divisore perchè $g(1)=1-2+2-1=0$,

ma a noi per la fattorizzazione interessa comunque dividere i due polinomi:

$$\begin{array}{cccc|l} x^3 & -2x^2 & +2x & -1 & x-1 \\ x^3 & -x^2 & & & x^2-x+1 \\ & -x^2 & +2x & -1 & \\ & -x^2 & +x & & \\ & & x & -1 & \\ & & & 0 & \end{array}$$

Abbiamo trovato che $g(x) = (x-1)\cdot(x^2-x+1)$, a questo punto verifichiamo se x^2-x+1 è riducibile o meno in $\mathbb{R}[x]$ attraverso il calcolo del delta: essendo negativo ($\Delta = 1-4 = -3$) il polinomio è irriducibile in $\mathbb{R}[x]$ e quindi la fattorizzazione cercata è proprio:

$$g(x) = (x-1)\cdot(x^2-x+1).$$

A questo punto per dimostrare che $x-1$ è un $M.C.D.(g(x), f_a(x))$ cominciamo mostrando che $x-1$ divide $f_a(x)$ per ogni $a \in \mathbb{R}$ (e quindi è un fattore comune). Basta osservare che $f_a(1) = 1-2a+2a-1 = 0$. Ora se mostriamo che x^2-x+1 non è un divisore di $f_a(x)$ per qualsiasi scelta di a in $\mathbb{R}$, abbiamo la tesi. Procediamo dunque calcolando il resto della divisione di $f_a(x)$ per x^2-x+1, che sarà un polinomio $r_a(x)$ che dipenderà dal coefficiente a. Dovremo osservare che $r_a(x)$ non è uguale al polinomio nullo qualsiasi sia la scelta di a in $\mathbb{R}$:

$$\begin{array}{cccccc|l} x^4 & & -2ax^2 & +2ax & -1 & & x^2-x+1 \\ x^4 & -x^3 & +x^2 & & & & x^2+x-2a \\ & x^3 & +x^2\cdot(-1-2a) & +2ax & -1 & & \\ & x^3 & -x^2 & +x & & & \\ & & -2a\cdot x^2 & +x\cdot(2a-1) & -1 & & \\ & & -2a\cdot x^2 & +2a\cdot x & -2a & & \\ & & & -x & -1+2a & & \end{array}$$

Osserviamo che il polinomio resto $r_a(x)$ è sempre di grado 1 qualsiasi sia la scelta di a in $\mathbb{R}$: in particolare non sarà mai uguale al polinomio nullo.

Esercizio 15.31. Dato il polinomio $g(x) = 4x^3+5x^2+3x+1$ fattorizzarlo in prodotto di irriducibili in $\mathbb{Q}[x]$ e in $\mathbb{Z}_{13}[x]$.

Risoluzione. Sappiamo che un polinomio di grado 3 è sicuramente riducibile in $\mathbb{R}[x]$ o in $\mathbb{C}[x]$, ma non conosciamo un algoritmo per trovare questa fattorizzazione. In $\mathbb{Q}[x]$ e in $\mathbb{Z}_p[x]$ un polinomio di grado 3 non sappiamo se è riducibile o no, ma abbiamo un algoritmo finito per rispondere a questa domanda e per trovare un'eventuale fattorizzazione in irriducibili del polinomio stesso. Questo perchè, come già osservato, la riducibilità di un polinomio di grado 3 è equivalente all'esistenza di una radice nel campo. Nel caso della riducibilità in $\mathbb{Q}[x]$ se il polinomio è a coefficienti interi (come $g(x)$) la Proposizione 15.27 permette di limitare le possibili radici razionali ad un insieme finito (tramite il calcolo dei divisori del termine noto e del coefficiente direttivo), mentre nel caso della riducibilità in $\mathbb{Z}_p[x]$ il numero delle possibili radici è ovviamente finito in quanto è finito il campo dei coefficienti.
I divisori del coefficiente direttivo sono $\{\pm 1, \pm 2 \pm 4\}$ mentre quelli del termine noto sono $\{\pm 1\}$, quindi le possibili radici razionali di $g(x)$ sono i numeri: $\{\pm\frac{1}{2}, \pm\frac{1}{4}, \pm 1\}$. Proviamoli, ma prima osserviamo che il polinomio $g(x)$ ha tutti coefficienti positivi e quindi non potrà avere radici positive. Ci possiamo dunque limitare a provare, tra le

possibili radici razionali, quelle negative:

$$g(-\tfrac{1}{4}) = -\tfrac{1}{16} + \tfrac{5}{16} - \tfrac{3}{4} + 1 = \tfrac{1}{2}$$
$$g(-1) = -4 + 5 - 3 + 1 = -1$$
$$g(-\tfrac{1}{2}) = -\tfrac{1}{2} + \tfrac{5}{4} - \tfrac{3}{2} + 1 = \tfrac{1}{4}$$

$g(x)$ non ha dunque radici razionali e quindi è irriducibile in $\mathbb{Q}[x]$.
Per quanto riguarda $\mathbb{Z}_{13}[x]$ valutando $g(x)$ per tutti gli elementi del campo si può verificare se esistono una o più radici. In questo caso troviamo $g(1) = 13 = 0$, quindi $g(x)$ è riducibile in $\mathbb{Z}_{13}[x]$ perché ha una radice e dunque per Ruffini è divisibile per $x - 1$:

$$\begin{array}{cccc|l} 4x^3 & +5x^2 & +3x & +1 & x-1 \\ 4x^3 & -4x^2 & & & 4x^2+9x+12 \\ & 9x^2 & +3x & +1 & \\ & 9x^2 & -9x & & \\ & & 12x & +1 & \\ & & 12x & -12 & \\ & & & +13 & \\ & & & 0 & \end{array}$$

Dunque $g(x) = (x-1)\cdot(4x^2+9x+12)$ in $\mathbb{Z}_{13}[x]$, si tratta di vedere se $4x^2+9x+12$ è irriducibile o meno in $\mathbb{Z}_{13}[x]$. Per questo si può procedere in due modi: o si provano tutti gli elementi di $\mathbb{Z}_{13}[x]$ alla ricerca di un'eventuale radice, oppure si usa la seguente osservazione:

Osservazione 15.32. La formula per la risoluzione delle equazioni di secondo grado vale in ogni campo $\mathbb{K}$ (e quindi in particolare per campi finiti).

Il Δ in questo caso è uguale a $81-192 = -111$ che in $\mathbb{Z}_{13}$ è equivalente a 6. Dobbiamo controllare se 6 è un quadrato in $\mathbb{Z}_{13}$:

$$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 = 3, 5^2 = 25 = 12, 6^2 = 10$$

E qui ci possiamo fermare perchè in $\mathbb{Z}_{13}$ $7 = -6$, $8 = -5$, $9 = -4$, $10 = -3$, $11 = -2$, $12 = -1$ e quindi i loro quadrati sono identici. Si può dunque concludere che 6 non è un quadrato in $\mathbb{Z}_{13}$ e quindi $4x^2+9x+12$ è irriducibile in $\mathbb{Z}_{13}[x]$.

Esercizio 15.33. Fattorizzare il polinomio $f(x) = x^5 + x^2 + 1$ in $\mathbb{Q}[x]$.

Risoluzione. Il polinomio $f(x)$ non ha radici in $\mathbb{Q}[x]$. Infatti dalla Proposizione 15.27 sappiamo che le uniche possibili radici razionali di $f(x)$ sono 1 e -1, ma valutando il polinomio in questi due valori si ottiene:

$$f(1) = 3 \quad f(-1) = 1$$

Il teorema di Ruffini ci dice dunque che $f(x)$ non ha fattori lineari in $\mathbb{Q}[x]$. A questo punto o $f(x)$ è irriducibile o è il prodotto di due polinomi irriducibili rispettivamente di secondo e terzo grado. Procediamo con il metodo della forza bruta (osserviamo che possiamo prendere i due eventuali polinomi fattore monici):

$$x^5 + x^2 + 1 = (x^3 + ax^2 + bx + c)(x^2 + dx + e) =$$
$$= x^5 + (a+d)x^4 + (e + ad + b)x^3 + (ae + bd + c)x^2 + (be + cd)x + ce$$

Abbiamo dunque il seguente sistema a coefficienti interi:

$$\begin{cases} a+d=0 \\ e+ad+b=0 \\ ae+bd+c=1 \\ be+cd=0 \\ ce=1 \end{cases}$$

Da $ce=1$ seguono due possibilità $c=e=1$ oppure $c=e=-1$, in entrambi i casi si ha $b=a=-d$. Sostituendo in $e+ad+b=0$ si ottiene, nel caso $e=1$:

$$a^2-a-1=0$$

e nel caso $e=-1$:

$$a^2-a+1=0$$

In entrambi i casi non esistono soluzioni intere. Dunque il metodo della forza bruta ci dice che il polinomio $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

Esercizio 15.34. Fattorizzare il polinomio $f(x)=x^4-1$ in $\mathbb{Z}_5[x]$.

Risoluzione. Il polinomio $f(x)$ ha 1 come radice, dunque per il teorema di Ruffini è divisibile per $x-1$. Osserviamo prima di proseguire che il risultato della divisione restituirà $f(x)$ come prodotto di $x-1$ per un polinomio $g(x)$ di terzo grado. Per completare la fattorizzazione di $f(x)$ dovremo dunque studiare la riducibilità di $g(x)$ che, essendo di terzo grado, è equivalente alla ricerca di radici in $\mathbb{Z}_5[x]$ del polinomio suddetto. Procediamo ora con la divisione di $f(x)$ per $x-1$:

$$\begin{array}{rrrrr|l}
x^4 & & & -1 & | & x-1 \\
x^4 & -x^3 & & & | & x^3+x^2+x+1 \\
 & x^3 & & -1 & | & \\
 & x^3 & -x^2 & & | & \\
 & & x^2 & -1 & | & \\
 & & x^2 & -x & | & \\
 & & & x \quad -1 & | & \\
 & & & x \quad -1 & | & \\
 & & & 0 & |
\end{array}$$

Dunque:

$$x^4-1=(x-1)\underbrace{(x^3+x^2+x+1)}_{g(x)}$$

Valutiamo se $g(x)$ ha radici in $\mathbb{Z}_5$:

$$g(0)=1 \quad g(1)=4 \quad g(2)=15=0 \quad g(3)=40=0 \quad g(4)=85=0$$

Perciò da Ruffini segue che $g(x)$ è fattorizzabile come:

$$g(x)=(x-2)(x-3)(x-4)$$

Concludendo:

$$f(x)=(x-1)(x-2)(x-3)(x-4)$$

Osserviamo che potevamo arrivare alla conclusione in maniera molto più rapida sfruttando le proprietà degli $\mathbb{Z}_p$ ed in particolare il piccolo teorema di Fermat. Infatti sappiamo che il polinomio x^5-x si annulla per ogni valore di $\mathbb{Z}_5$ e basta osservare che:

$$x^5-x=x(x^4-1)$$

Ovvero x^4-1 si annulla in tutti gli elementi di $\mathbb{Z}_5$ tranne che in 0 e dunque è fattorizzabile proprio come:

$$f(x) = (x-1)(x-2)(x-3)(x-4)$$

Esercizio 15.35. Sia $p(x) = x^4 - 4x^3 + 6x^2 - 4x + 5$. Sapendo che $2+i$ è una radice complessa del polinomio $p(x)$ fattorizzarlo in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$.

Risoluzione. Se $\alpha = 2+i$ è radice, allora (Proposizione 15.19) anche il suo complesso coniugato $\overline{\alpha} = 2-i$ è radice di $p(x)$. Dunque il polinomio è divisibile per:

$$(x-(2+i))(x-(2-i)) = (x-2)^2 - i^2 = x^2 - 4x + 4 + 1 = x^2 - 4x + 5$$

Eseguiamo la divisione:

$$\begin{array}{cccccc|l} x^4 & -4x^3 & +6x^2 & -4x & +5 & | & x^2-4x+5 \\ x^4 & -4x^3 & +5x^2 & & & | & x^2+1 \\ & & x^2 & -4x & +5 & | & \\ & & x^2 & -4x & +5 & | & \\ & & & & 0 & | & \end{array}$$

Abbiamo dunque trovato che:

$$p(x) = (x^2 - 4x + 5)(x^2 + 1)$$

che è la fattorizzazione in irriducibili in $\mathbb{R}[x]$, infatti entrambi i polinomi di secondo grado non hanno soluzioni reali. Visto che x^2+1 ha come radici complesse i e $-i$ la fattorizzazione in irriducibili di $p(x)$ in $\mathbb{C}[x]$ è:

$$p(x) = (x-(2+i))(x-(2-i))(x-i)(x+i)$$

Esercizio 15.2. Fattorizzare il polinomio $x^4 + 4x^3 - 19x^2 + 8x - 42$ come prodotto di irriducibili in $\mathbb{R}[x],\ \mathbb{Q}[x],\ \mathbb{Z}_3[x],\ \mathbb{Z}_{13}[x]$.

Esercizio 15.3. Fattorizzare il polinomio $x^4 - 4x^3 + x^2 + 8x - 6$ come prodotto di irriducibili in $\mathbb{R}[x],\ \mathbb{Q}[x],\ \mathbb{Z}_7[x],\ \mathbb{Z}_{11}[x]$.

Esercizio 15.4. Consideriamo il polinomio

$$p(x) = x^4 - x^3 - x^2 - x - 2$$

Fattorizzare $p(x)$ come prodotto di irriducibili in$\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_3[x]$.

Esercizio 15.5. Fattorizzare il polinomio $f(x) = x^6 - x^5 - 2x^4 - 2x^2 + 2x + 4$ come prodotto di irriducibili in $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$, $\mathbb{Z}_2[x], \mathbb{Z}_3[x]$.

Esercizio 15.6. Dimostrare che per ogni $p \in \mathbb{N}$ primo, il polinomio:

$$\sum_{i=0}^{p-1} x^i$$

è irriducibile in $\mathbb{Q}[x]$.