1

Capitolo B25

induzione matematica, aritmetica modulare, terne pitagoriche

Contenuti delle sezioni

23 pagine

B250.01 Dopo aver introdotto lo schema di induzione matematica in relazione con la successione dei numeri naturali, si studiano le prime proprietà dei numeri primi, a cominciare dal fatto che costituiscono un insieme numerabile e dalla possibilità di fattorizzare mediante primi ogni intero positivo.

Successivamente si esaminano le congruenze tra numeri interi e, in relazione a ciascuno degli interi m maggiori o uguali a 2, si studia l'insieme $\mathbb{Z}_m$ delle classi di resti modulo m.
Su queste classi si definiscono le operazioni di somma e prodotto che consentono di attribuire agli $\mathbb{Z}_m$ una struttura che in algebra si assegna alla specie degli anelli uniferi commutativi e si esamina la possibilità di definire su alcune di queste strutture algebriche una operazione di divisione.

Si stabilisce che si ha l'invertibilità di tutti gli elementi di una $\mathbb{Z}_m$, ad esclusione del suo elemento nullo, sse m è un numero primo p.
Questo consente di attribuire agli $\mathbb{Z}_p$ una struttura algebrica della specie che in algebra è chiamata cam; nell'ambito di ciascuno di questi camp si possono introdurre varie costruzioni e varie proprietà di grande portata.

Sono poi esaminate le terne pitagoriche, terne di numeri positivi che risulteranno utili allo sviluppo della impostazione costruttiva della geometria che inizieremo con l'esame dalle caratteristiche del piano-QQ [B30].

Nell'ultima parte vengono esaminate alcune classiche funzioni aritmetiche, funzioni che a ogni intero positivo associano un intero, e con esse alcune classiche successioni di numeri interi.

B25 a. schema di induzione matematica

B25a.01 Per **schema di induzione matematica** intendiamo uno schema di dimostrazione, garantito da un'affermazione, chiamata spesso **principio di induzione matematica**; questo schema è utilizzato per una grande varietà di dimostrazioni, ciascuna delle quali riguardante un insieme numerabile di enunciati che nei casi più semplici si riesce facilmente e significativamente a porre in corrispondenza biunivoca con l'insieme dei numeri naturali.

Questo schema può essere formulato in diversi modi, alcuni essenzialmente equivalenti, altri più differenziati e aventi diversa portata.

La prima formulazione dello schema di induzione che esaminiamo riguarda una successione di affermazioni $\langle P(0), P(1), ..., P(n), ...\rangle$, nella n-esima delle quali compare il numero naturale n, e ha come fine la dimostrazione della tesi della forma

(1) $$\mathcal{T} \;:=\; \lceil \forall n \in \mathbb{N} \;:\; P(n) \rceil \;.$$

Le schema prevede che si affrontino due stadi dimostrativi:

[1] Si dimostra che vale $P(0)$.

[n] Si avanza l'ipotesi che valga l'asserto $P(n)$ per un imprecisato intero naturale n e da questa si deduce che vale anche l'asserto $P(n+1)$.

Quando si sono conclusi i due stadi dimostrativi si considera che sia stata raggiunta la tesi (1).

In genere lo stadio [1] viene chiamato **base dell'induzione** e lo stadio [n] **passo induttivo**; l'ipotesi che valga l'asserto $P(n)$ per un generico $n \in \mathbb{N}$ viene detta **ipotesi induttiva**.

B25a.02 Prima di fornire una giustificazione dello schema di induzione sopra enunciato, conviene segnalare quanto segue, anticipando per sommi capi alcuni contenuti di B65.

Secondo la logica matematica la dimostrazione di una proposizione $\mathcal{P}$ della forma $\mathcal{P} \;:=\; \lceil \mathcal{I} \Longrightarrow \mathcal{T} \rceil$ consiste in una catena deduttiva, cioè in una sequenza di enunciati che inizia con gli enunciati $\mathcal{I}$ costituenti le ipotesi della $\mathcal{P}$ e si conclude con gli enunciati costituenti la sua tesi $\mathcal{T}$.

Ogni nuovo enunciato della catena si ottiene facendo operare sopra uno o più enunciati trovati in precedenza le cosiddette **regole di deduzione**; queste sono meccanismi di trasformazione formale degli enunciati, meccanismi che hanno in precedenza ottenuto una qualche "garanzia di validità" nell'ambito della teoria sviluppata all'interno della logica matematica che si assume come campo di validità della $\mathcal{P}$.

Lo schema di induzione prevede che si precisi una catena deduttiva che dalle ipotesi $\mathcal{I}$ giunga a $P(0)$ e di una catena deduttiva che dalle ipotesi ampliate con l'enunciato $P(n)$ ottenga l'enunciato $P(n+1)$, cioè che dimostri la $\lceil \mathcal{I} \wedge P(n) \implies P(n+1) \rceil$.
Per ottenere la dimostrazione di un enunciato $\mathcal{P}$ si può dunque organizzare una **procedura di induzione matematica** con il compito di generare gli enunciati che seguono.

A partire dalle ipotesi $\mathcal{I}$ dimostra la validità di $P(0)$.

A partire da $\mathcal{I}$, da $P(0)$ e da $\lceil P(n) \Longrightarrow P(n+1) \rceil$ dimostra $P(1)$.

A partire da $\mathcal{I}$, da $P(1)$ e da $\lceil P(n) \Longrightarrow P(n+1) \rceil$ dimostra $P(2)$.

A partire da $\mathcal{I}$, da $P(2)$ e da $\lceil P(n) \Longrightarrow P(n+1) \rceil$ dimostra $P(3)$.

. . . . . .

Se si assume della disponibilità delle risorse computazionali illimitate [B18a] risulta lecito affermare che la precedente procedura può operare quanto si vuole, in modo che, proposto un arbitrario $N \in \mathbb{P}$ si riesca a ottenere la dimostrazione di $P(N)$.
In termini più effettivi, quando si dovesse garantire l'enunciato $P(N)$ per un certo $N \in \mathbb{N}$, se le risorse lo permettono, si può ottenere la sua dimostrazione, cioè una sua catena deduttiva (finita).
Questo si può esprimere concisamente con la frase "L'enunciato $P(N)$ vale per ogni N intero positivo" e con la scrittura concisa $\forall N \in \mathbb{N} \ : \ P(N)$. Questa frase e questa espressione presentano il vantaggio di essere riutilizzabili per i successivi sviluppi senza dovere entrare nel merito delle potenzialmente infinite procedure relative ad $N = 1, 2, 3, ...$ che dovrebbero giustificarla.

B25a.03 Il primo utilizzo documentato dello schema di induzione è dovuto a Maurolico e compare nel suo testo *Arithmeticorum libri duo* del 1575. Qui egli dimostra che la somma dei primi $n + 1$ interi dispari è uguale a $(n + 1)^2$.

Per questo si considera la successione delle proposizioni alla m-esima delle quali si può dare la forma

$$P(m) \ := \ \left\lceil \sum_{h=0}^{m} (2h + 1) \ = \ (m + 1)^2 \right\rceil \ .$$

La base dell'induzione è $\displaystyle\sum_{h=0}^{0}(2h + 1) \ = \ 1$, evidentemente valida.
Il passo induttivo chiede di dimostrare

$$\sum_{h=0}^{m}(2h + 1) \ = \ (m + 1)^2 \implies \sum_{h=0}^{m+1}(2h + 1) \ = \ (m + 2)^2 \ .$$

In effetti $\displaystyle\sum_{h=0}^{m+1}(2h + 1) \ = \ \sum_{h=0}^{m}(2h + 1) + 2(m + 1) + 1 \ = \ (m + 1)^2 + 2(m + 1) + 1 \ = \ (m + 2)^2$.
Risulta quindi dimostrato che, per qualsiasi n intero positivo

$$\sum_{h=0}^{n} (2h + 1) \ = \ (n + 1)^2 \ .$$

B25a.04 Come preannunciato dello schema di induzione matematica si possono presentare diverse varianti e ciascuna di esse risulta meglio utilizzabile in un determinato insieme di circostanze.

Una prima variante riguarda una base dell'induzione concernente un intero iniziale diverso da 0.

Per un dato numero intero k, si considerano proposizioni $Q(m)$ per $m = k, k + 1, k + 2, ...$ Quindi si effettuano i due stadi dimostrativi che seguono.

[1] Dall'ipotesi iniziale si deduce che vale $Q(k)$.
[2] Aggiungendo all'ipotesi iniziale $\mathcal{I}$ la richiesta che valga l'asserto $Q(n)$ per un generico intero $n \geq k$ e si dimostra che vale anche $Q(n + 1)$.

Si può concludere che vale $Q(m)$ per ogni $m \in \mathbb{N} + k$.

Questo schema risulta strettamente equivalente al precedente definendo per ogni m intero naturale la proposizione $P(m) := Q(m - k)$; in altre parole si ottiene dal primo operando una traslazione di passo k degli indici che individuano le affermazioni.

Questa formulazione viene utilizzata spesso per $k = 1$, talvolta per $k = -1$ (ad esempio per trattare la `successione di Fibonacci (wi)`), talvolta per $k = 3$ (ad esempio per proprietà riguardanti poligoni piani).

B25a.05 Un'altra variante viene detta **schema di induzione matematica forte**.

Per un certo m intero positivo si prendono in esame gli enunciati $R(0)$, $R(1)$, $R(2)$, ... , $R(m)$.

Si effettuano i due stadi dimostrativi:

[1] A partire da $\mathcal{I}$ si deduce che valgono $R(0)$, $R(1)$,...,$R(m)$.

[2] Per un qualsiasi $n = m, m+1, m+2, ...$ a partire da $\mathcal{I}$ e dagli asserti $R(0), R(1), ..., R(n)$ si dimostra che vale anche $R(n+1)$.

Si può concludere che $\forall n \in \mathbb{N} \ : \ R(n)$.

Questo schema si riduce al primo definendo per ogni m intero naturale la proposizione

$$P(m) \ := \ ⌈ \text{ Valgono } R(0), R(1), \text{ ... ed } R(m) ⌉ \ .$$

In altre parole si passa a una successione di affermazioni ciascuna delle quali costituisce la disgiunzione di tutte le precedenti.

Si osserva che questo schema in molti casi consente dimostrazioni per induzione più agevoli, in quanto rende disponibile per il passo induttivo una ipotesi più incisiva.

B25a.06 Occorre notare che lo schema di induzione qui è stato introdotto secondo una visione procedurale che può essere giudicata piuttosto intuitiva. Questo schema di induzione può essere collocato entro esposizioni più formalmente elaborate che si basano su sistemi di assiomi ben definiti.
Secondo alcune di queste esposizioni viene considerato come un teorema, mentre secondo altre viene assunto come un assioma.

Si dimostra in particolare che lo schema di induzione equivale al cosiddetto **principio di buon ordinamento** per i numeri naturali. Questo afferma che ogni sottoinsieme dell'insieme $\mathbb{N}$ contiene il suo elemento minimo e costituisce un insieme bene ordinato.

Segnaliamo che lo schema di induzione si può formulare anche per proposizioni che risulta naturale associare, non ai numeri naturali, ma a una famiglia (numerabile) di enunciati indicizzabili con gli elementi di qualche insieme generabile-iop [B30a01] dotato di una struttura più articolata di quella sequenziale di $\mathbb{N}$.

Esso per esempio può essere formulato per proposizioni associate a nodi di un digrafo infinito, dotato di un nodo radice, cioè di un nodo dal quale sono raggiungibili tutti gli altri mediante un insieme finito di ben definite operazioni di passaggio da un nodo (o da un opportuno raggruppamento di nodi) a un altro [D28].

In particolare vari casi interessanti riguardano proposizioni associate ai nodi di un'arborescenza infinita [D30] e, ancora più in particolare, riguardano enunciati associati alle stringhe di un linguaggio formale generabile-iop [C12, C14].

Altri casi di possibile applicazione si incontano nello studio dei circuiti-ZZ-or limitati sul piano $\mathbb{Z} \times \mathbb{Z}$, dei circuiti-QQ-or limitati sul piano $\mathbb{Q} \times \mathbb{Q}$ e i circuiti orientati con nodi sul piano $\mathbb{Q}_{\mathsf{C}} \times \mathbb{Q}_{\mathsf{C}}$.

B25a.07 **(1) Eserc.** Dimostrare per induzione che la formula $\binom{n}{k} = \dfrac{n(n-1)\cdots(n-k+1)}{k!}$ fornisce valori interi positivi. Più in generale dimostrare che il prodotto di n interi positivi successivi è divisibile per n fattoriale.

(2) Eserc. Dimostrare che se n è un intero dispari $n^2 - 1$ è multiplo di 8.

(3) Eserc. Dimostrare che per ogni n intero $n^3 - n$ è divisibile per 6.

(4) Eserc. Dimostrare che per ogni n intero positivo $3^{2n} - 2^n$ è divisibile per 7.

(5) Eserc. Dimostrare che per $n = 4, 5, 6, ...$ il numero delle diagonali di un poligono convesso di n lati è $\dfrac{n(n-3)}{2}$.

B25 b. congruenze tra numeri interi

B25b.01 Per giungere ad alcune conclusioni generali risulta utile servirsi di operazioni che hanno come operandi insiemi di numeri interi; tra queste vi sono le cosiddette estensioni booleane delle operazioni aritmetiche.

Consideriamo quindi A, B e C generici sottoinsiemi di $\mathbb{Z}$.

Si dice **estensione booleana della somma di interi** l'operazione che a due sottoinsiemi A e B di $\mathbb{Z}$ associa

$$A +^{be} B \;:=\; \{a \in A, b \in B :|\; a+b\} \;.$$

Si dice **estensione booleana della differenza di interi** l'operazione che ad $A, B \subseteq \mathbb{Z}$ associa

$$A -^{be} B \;:=\; \{a \in A, b \in B :|\; a-b\} \;.$$

Si dice **estensione booleana del prodotto di interi** l'operazione che ad $A, B \subseteq \mathbb{Z}$ associa

$$A \cdot^{be} B \;:=\; \{a \in A, b \in B :|\; a \cdot b\} \;.$$

Definizioni simili si possono dare per quoziente, resto, massimo comun denominatore e minimo comune multiplo.

B25b.02 In genere è semplice costruire gli insiemi forniti dalle estensioni booleane delle varie operazioni quando sono applicate a insiemi operandi finiti. Alcuni esempi:

$\{2,7,12\} +^{be} \{3,5\} \;=\; \{5,7,10,12,15,17\}$, $\quad \{2,7,12\} -^{be} \{3,5\} \;=\; \{-3,-1,2,4,7,9\}$,

$\{2,7,12\} \cdot^{be} \{3,5\} \;=\; \{6,10,21,35,36,60\}$.

La valutazione è particolarmente semplice se uno dei due insiemi operandi si riduce a un singoletto: $\{4\} \cdot^{be} \{5,15,25\} = \{20,60,100\}$.
Eseguire manualmente questa manovra sopra due insiemi finiti estesi e "poco regolari" può essere molto tedioso.

Quando invece uno o entrambi gli operandi sono insiemi infiniti la valutazione dipende dalla modalità di individuazione di ogni operando infinito e l'individuazione dell'insieme risultato può essere impegnativa.

Un esempio semplice è

$$\{3,5,7\} \cdot^{be} \{n \in \mathbb{P} :|\; 13\,n\} \;=\; \{39,65,78,91,117,130,156,195,234,260,273,312,325,...\} \;;$$

Esso suggerisce che l'aspressione a sinistra può essere la più utile.

In genere le notazioni per le estensioni booleane vengono semplificate senza incorrere in ambiguità che non possano essere risolte ponendo attenzione al contesto.
Oltre a sostituire " $+^{be}$ ", " $-^{be}$ " e " $\cdot^{be}$ " con i semplici segni " $+$ ", " $-$ " e " $\cdot$ " spesso il segno di prodotto si omette e si semplifica la scrittura degli insiemi costituiti da un soli intero trascurando le parentesi graffe.
Un insieme come $\{4\} \cdot^{be} \{5,15,25\}$ si può segnalare scrivendo semplicemente $4\{5,15,25\}$; invece di $\{0\} -^{be} B$ si scrive solo $-B$.

Osserviamo che in generale $A - A = \{0\}$ sse A è un singoletto: invece $\{4,7\} - \{4,7\} = \{-3,0,3\}$ e $\{1,4,9\} - \{1,4,9\} \;=\; \{-8,-5,-3,0,3,5,8\}$.

Queste relazioni suggeriscono di dimostrare che sottraendo un insieme di interi da se stesso si ottiene un sottoinsieme di $\mathbb{Z}$ invariante per cambiamento di segno. In effetti possiamo affermare

$$\forall I \subset \mathbb{Z} \;:\; \; -(I-I) \;=\; (I-I) \quad \text{ovvero} \quad \forall I \subset \mathbb{Z} \;:\; \mathsf{Mirr}_{[0]}(I-I) \;=\; I-I \;.$$

B25b.03 Denotiamo con m un intero maggiore o uguale a 2 e ricordiamo che $m \cdot \mathbb{Z}$ esprime l'insieme degli interi multipli di m.
Se inoltre $h \in \mathbf{[}m\mathbf{)}$, con $m \cdot \mathbb{Z} + h$ si denota l'insieme degli interi ottenuti aggiungendo h ai multipli di m.
Per esempio $3 \cdot \mathbb{Z} + 7 \ = \ \{..., -5 - 2, 1, 4, 7, 10, 13, 16, 19, ...\}$.
Similmente $m \cdot \mathbb{N}$ denota l'insieme dei multipli naturali di m e $m \cdot \mathbb{P}$ denota l'insieme dei multipli positivi di m.

Per ogni $t \in \mathbb{Z}$ ed $r \in \mathbb{P}$ l'insieme della forma $t + r \cdot \mathbb{N}$ viene chiamato **progressione aritmetica** con primo termine t e ragione r.

Ricordiamo che in varie circostanze è utile tenere presente la bipartizione di $\mathbb{Z}$ nell'insieme degli interi pari e nell'insieme dei dispari esprimibile con la formula

$$\mathbb{Z} \ = \ 2 \cdot \mathbb{Z} \ \dot\cup \ 2 \cdot \mathbb{Z} + 1 \ .$$

Con la definizione che segue procediamo a generalizzare questa bipartizione con una partizione di $\mathbb{Z}$ in m parti, per un qualsiasi m maggiore o uguale a 2.

Due interi i_1 e i_2 si dicono **interi congruenti modulo** m sse $i_1 - i_2$ è multiplo di m. Per esprimere questo fatto si scrive di solito $i_1 \equiv i_2 \pmod m$.
Qui per la relazione di congruenza modulo m proponiamo come più chiara la notazione $i_1 \ =_m \ i_2$.
Abbiamo quindi l'enunciato che si può assumere come definizione della relazione "$=_m$" :

$$\forall i_1, i_2 \in \mathbb{Z} \ \ : \ \ i_1 \ =_m \ i_2 \iff (i_1 - i_2) \in m\mathbb{Z} \ .$$

B25b.04 **Prop.** La relazione di congruenza modulo m è una equivalenza entro $\mathbb{Z}$.

Dim.: Chiaramente $\forall i \in \mathbb{Z} : \ i =_m i$, ossia $=_m$ è una relazione riflessiva.
Essa inoltre è simmetrica in quanto $i_1 =_m i_2 \iff i_1 - i_2 \in m\mathbb{Z} \iff i_2 - i_1 \in m\mathbb{Z} \iff i_2 =_m i_1$.
Infine $=_m$ è transitiva in forza delle relazioni: $i_1 =_m i_2$, $i_2 =_m i_3 \implies$
$i_1 - i_3 \ = \ (i_1 - i_2) + (i_2 - i_3) \ = \ h_1 m + h_2 m \ = \ (h_1 + h_2)m \iff (i_1 - i_3) \in m\mathbb{Z} \iff i_1 =_m i_3$ ∎

B25b.05 Esaminiamo le classi delle equivalenze espresse da $=_m$. Una di queste è $m\mathbb{Z}$, l'insieme dei multipli di m, cioè l'insieme degli interi congrui modulo m a 0. In generale, per qualsiasi $h \in \mathbf{[}m\mathbf{)} = \{0, 1, 2, ..., m-1\}$, la **classe di congruenza modulo** m di h è costituita dagli interi i per i quali accade che $i - h = km$ per qualche intero k, cioè è costituita dagli interi ottenibili sommando h a un multiplo di m, ovvero viene espressa da $m\,\mathbb{Z} + h$.

Per questa classe di congruenza adottiamo anche la notazione $[h]_m$. L'intero h è un rappresentativo di tale classe e un insieme significativo di rappresentativi delle varie classi è

(1) $$[h]_m \ \text{ corrisponde a } \ \mathbf{[}m\mathbf{)} \ = \ \{0, 1, ..., m-1\}.$$

Una classe di congruenza modulo m si può individuare anche come $[k]_m$ con k intero qualsiasi, non necessariamente appartenente a $\mathbf{[}m\mathbf{)}$.

Per esempio $[1]_5 \ = \ \{...-19, -14, -9, -4, 1, 6, 11, 1621, 26, ...\} \ = \ [1001]_5$ e le tre classi di congruenza modulo 3 si possono denotare $[-1]_3$, $[0]_3$, $[1]_3$. La notazione (1) precedente con $h \in \mathbf{[}m\mathbf{)}$ va considerata forma canonica.

Talora è utile individuare le classi di resti con interi negativi piccoli, appartenenti a intervalli del tipo $\mathbf{(}-m : 0\mathbf{]}$. Per esempio per $m = 2$, si hanno le classi $[0]_2$ e $[1]_2 = [-1]_2$, mentre per $m = 7$, si hanno le classi $[0]_7$, $[1]_7 = [-6]_7$, $[2]_7 = [-5]_7$, $[3]_7 = [-4]_7$, $[4]_7 = [-3]_7$, $[5]_7 = [-2]_7$, $[6]_7 = [-1]_7$.,

Le 10 classi di congruenza modulo 10 $[h]_{10}$ per $h = 0, 1, ..., 9$ sono costituite, risp., dagli interi naturali che nella notazione decimale presentano la stessa ultima cifra h e contengono, risp., gli interi negativi che presentano la stessa ultima cifra $10 - h$: ad esempio $[7]_10 \ = \ \{..., -23, -13, -3, 7, 17, 27, ...\}$.

B25b.06 Le classi di congruenza modulo m sono dette anche **classi di resti modulo** m, termine che rispecchia il fatto che un intero positivo i appartiene alla classe di congruenza modulo m individuata dal resto della divisione tra lo stesso intero positivo i e l'intero positivo m.

L'insieme di classi di congruenza avente la forma $\{[0]_m, [1]_m, ...[m-1]_m\}$ si dice anche **quoziente dell'insieme** $\mathbb{Z}$ rispetto al suo sottoinsieme $m\mathbb{Z}$ e si denota con $\mathbb{Z}/m\mathbb{Z}$ o anche con $\mathbb{Z}/ =_m$.
Spesso risulta comoda anche la notazione $\mathbb{Z}_m \ := \ \mathbb{Z} \,/\, m\mathbb{Z}$.

Si ha quindi la formula della partizione di $\mathbb{Z}$ nelle m classi di congruenza modulo m

$$\mathbb{Z} \ = \ [0]_m \,\dot\cup\, [1]_m \,\dot\cup\, \cdots \,\dot\cup\, [m-1]_m \ = \dot{\bigcup}_{h=0}^{m-1} \ m\mathbb{Z} + h \ .$$

In particolare $\mathbb{Z} \ = \ [0]_3 \,\dot\cup\, [1]_3 \,\dot\cup\, [2]_3$.

B25b.07 La formula precedente si può illustrare con la presentazione di $\mathbb{Z}$ in forma di matrice con infinite righe di lunghezza m come nel caso seguente relativo a $m = 12$

$$\begin{array}{cccccccccccc}
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
-24 & -23 & -22 & -21 & -20 & -19 & -18 & -17 & -16 & -15 & -14 & -13 \\
-12 & -11 & -10 & -9 & -8 & -7 & -6 & -5 & -4 & -3 & -2 & -1 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 \\
24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}$$

Le 12 classi di resti corrispondono alle successive colonne e la precedente formula di ripartizione alla presentazione della matrice degli elementi di $\mathbb{Z}$ come affiancamento delle sue colonne.

B25b.08 Un'altra utile presentazioni delle classi di resti si può pensare ottenuta "avvolgendo" la retta-Z su una circonferenza in grado di accogliere m archi di lunghezza pari a 1, cioè su una circonferenza di lunghezza m e quindi di raggio uguale a $\dfrac{m}{2\,\pi}$.
Nei casi $m = 5$ e $m = 8$ si ottiene

//input pB25b08

La precedente figura mostra chiaramente come la congruenza possa servire a trattare fenomeni periodici come il succedersi delle 24 ore nelle giornate o il succedersi dei 7 giorni nelle settimane.
Si osserva che un fenomeno meno convenzionale come il succedersi dei giorni negli anni viene presentato con una periodicità che richiede correzioni, interventi non semplici come dimostra la complessa storia dei calendari.

Si osserva anche che sugli insiemi $\mathbb{Z}_m$ non si impone un ordinamento lineare, ma è più utile un cosiddetto **ordinamento ciclico**, relazione costituita dalle coppie $\langle [h]_m, [h+1]_m \rangle$ per $h = 0, 1, ..., m-1$.

Le figure del tipo precedente si dicono **raffigurazioni cicliche** delle congruenze modulari.

B25b.09 **Prop.** Per ogni intero $m = 2, 3, ...$ e per gli interi arbitrari i_1, i_2, j_1 e j_2 si ha:

$$i_1 =_m i_2 \ \ , \ \ j_1 =_m j_2 \ \ \Longrightarrow \ \ i_1 + j_1 \ =_m \ i_2 + j_2 \ \ , \ \ i_1 \cdot j_1 \ =_m \ i_2 \cdot j_2 \ .$$

Dim.: Supponiamo di avere $i_2 - i_1 =: h\,m$ e $j_2 - j_1 =: k\,m$. Per la somma si trova
$(i_1 + j_1) - (i_2 + j_2) \;=\; (i_1 - i_2) + (j_1 - j_2) \;=\; mh + mk \;=\; m(h + k)$, cioè $i_1 + j_1 \;=\; {}_m i_2 + j_2$.
Per il prodotto si trova invece:
$i_1 \cdot j_1 - i_2 \cdot j_2 \;=\; (i_1 - i_2) \cdot j_1 - i_2 \cdot (j_2 - j_1) \;=\; mhj_1 + i_2 mk \;=\; m(hj_1 + kj_2)$, cioè $i_1 \cdot j_1 \;=_m\; i_2 \cdot j_2$ ∎

Il risultato precedente si esprime anche dicendo che le operazioni di somma e prodotto tra interi **rispettano le classi della congruenza** modulo m.

B25**b.10** Questo risultato consente di trovare la classe di congruenza di un intero i grande ma fornito come prodotto di numeri interi più piccoli evitando di calcolo di i tendenzialmente faticoso.

Il vantaggio è particolarmente evidente quando, come spesso accade, si opera manualmente e con notazioni decimali e quando interessano classi di congruenza come quelle modulo 2, 3, 4, 5, 10, 20, 25, 50, 100 e 1000.

Alcuni esempi di questi calcoli sveltiti sono forniti dai seguenti sviluppi:

$[5273 \cdot 7803]_3 \;=\; [5273]_3 \cdot [7803]_3 \;=\; [2]_3 \cdot [1]_3 \;=\; [2]_3$.

$[347228 \cdot 34754]_{25} \;=\; [347228]_{25} \cdot [34754]_{25} \;=\; [3]_{25} \cdot [4]_{25} \;=\; [12]_{25}$.

Nelle espressioni esaminabili in questo modo possono intervenire delle sottrazioni: per queste basta tenere conto che $-k =_m m - k$.

B25**b.11** Dalle considerazioni precedenti si ricava immediatamente un criterio necessario che presenta una certa utilità quando occorre controllare la correttezza di calcoli sui numeri interi.

(1) Prop.: Consideriamo una uguaglianza della forma $E = v$, dove E denota una espressione polinomiale (cioè una espressione contenente somme, ottrazioni e prodotti) su operandi interi e v è un intero.
Condizione necessaria, ma non sufficiente, per la validità dell'espressione è la validità di una espressione $[E]_m = [v]_m$ per qualche $m = 2, 3, \ldots$ ∎

Questo criterio può essere utile quando la valutazione di $[E]_m$ è molto meno gravosa della valutazione di E.
In particolare si può verificare rapidamente se una uguaglianza della forma $E = v$ rispetta o meno la parità, la congruenza modulo 10, la congruenza modulo 100 e la congruenza modulo 3.

B25**b.12** Sulle considerazioni precedenti si basa anche la tradizionale "prova del 9".
Essa riguarda l'applicazione del precedente criterio sufficiente nel caso $m = 9$ e di uguaglianze della forma $f \cdot g = v$ con f e g notazioni decimali di interi positivi e inoltre si serve del seguente fatto che consente di semplificare i calcoli delle classi di congruenza modulo 9.

(1) Prop.: Consideriamo $i \in \mathbb{P}$ e si disponga della sua rappresentazione decimale

$$i \;=:\; i_p \cdot 10^p + i_{p-1} \cdot 10^{p-1} + \cdots + i_1 \cdot 10 + i_0 \;;$$

vale l'uguaglianza modulare $[i]_9 = [i_p + i_{p-1} + \cdots + i_1 + i_0]_9$.

Dim.: Dalle definizioni segue

$$i - (i_p + i_{p-1} + \cdots + i_1 + i_0) \;=\; i_p \cdot (10^p - 1) + i_{p-1} \cdot (10^{p-1} - 1) + \cdots + p_1 \cdot (10 - 1) + p_0 \cdot (1 - 1)$$

e ciascuno dei fattori $10^q - 1$ è multiplo di 9 ed è algoritmicamente precisabile ∎

La proposizione precedente consente di servirsi, anche reiteratamente, della funzione M_9 che ha come dominio l'insieme delle scritture decimali dei numeri naturali e come codominio $[9)$ e che viene definita dalle richieste seguenti:

$$M_9(i) \;:=\; i \;\text{ se }\; i \in [0:8] \qquad := 0 \;\text{ se }\; i = 9 \qquad := M_9\,(M_9(i)) \;\text{ se }\; i = 10, 11, \ldots \;.$$

Per esempio si calcola $M_9(3\,850\,721) = M_9(26) = M_9(8) = 8$.

Le seguenti uguaglianze modulari consentono di sveltire ulteriormente il calcolo della M_9.

Per ogni $h \in \mathbb{N}$ si ha $[h \pm 9 \cdot 10^h]_9 \;=\; [h]_9$;

per ogni $h, k \in \mathbb{P}$ con $h < k$ si ha $[10^k - 10^h]_9 = [10^h(10^{k-h} - 1)]_9 = 0$;

per ogni $h, k \in \mathbb{P}$ con $h < k$, per ogni $j \in \mathbb{P}$ e per ogni $c \in [1 : 8]$ si ha
$$[j + c(10^k - 10^h)]_9 = [j + c \cdot 10^h(10^{k-h} - 1]_9 = [j]_9 \;;$$
per ogni $h, k \in \mathbb{P}$ con $h < k$, per ogni $j \in \mathbb{P}$ e per ogni $c \in [1 : 8]$ si ha
$$[j + c \cdot 10^k + (9 - c) \cdot 10^h]_9 = [j - 9 \cdot 10^h + c \cdot (10^k - 10^h)]_9 = [j]_9 \;.$$

Di conseguenza il calcolo di un $M_9(i)$ può essere sveltito eliminando dalla stringa costituente il suo argomento le occorrenze di 0 e 9 o i duetti di occorrenze di cifre aventi come somma 9 (8+1, 7+2, 6+3, 5+4), anche se le due cifre addende non sono adiacenti.

Per esempi $M_9(38\,507\,912) \;=\; M_9(385\,712) \;=\; M_9(3\,851) \;=\; M_9(35) \;=\; 8$.

B25b.13 **Eserc.** Estendere la "prova del 9" a una "prova del $B - 1$" per i calcoli su numeri interi positivi condotti su notazioni posizionali in base B, con $B = 2, 3, \ldots$. È consigliabile la definizione di una funzione M_B che generalizza la M_9.

B25 c. operazioni aritmetiche sulle classi di resti

B25c.01 La b09 garantisce che le operazioni di somma e prodotto applicate a classi di resti modulo m portano ad altre classi di resti modulo m:

$$[a]_m +^{be} [b]_m \;=\; [a+b]_m \qquad , \qquad [a]_m \cdot^{be} [b]_m \;=\; [a\cdot b]_m \;. \tag{1}$$

A queste uguaglianze possiamo aggiungere quelle riguardanti cambiamento di segno e sottrazione

$$-^{be} [a]_m \;=\; [m-a]_m \qquad , \qquad [a]_m -^{be} [b]_m \;=\; [a+m-b]_m \;=\; [a-b]_m \;. \tag{2}$$

Di conseguenza possiamo trattare le operazioni di somma, prodotto, differenza e cambiamento di segno modulo m all'interno di ciascuno degli insiemi $\mathbb{Z}_m$.

Gli enunciati sulle classi di resti e sulle relative operazioni spesso si possono esprimere con varie semplificazioni.
Come si è detto di solito le estensioni booleane delle operazioni su numeri si esprimono con i semplici segni " + ", " · " e " − "; inoltre il segno di prodotto spesso può essere omesso.

Nei brani nei quali Quando m può essere considerato implicito le classi di resti $[a]_m$, $[b]_m$, ... si possono individuare semplicemente con a, b, ... e invece di scrivere $a =_m b$ si scrive $a = b$.
Per esempio dove risulta chiaro che si stanno trattando le classi di resti modulo 7 diventa lecito usare scritture $5 + 6 = 4$ e $3 \cdot 5 = 1$.

All'opposto in un brano espositivo nel quale si trattano sia classi di resti modulo 7 che classi di resti modulo 12 si dovrebbero presentare enunciati come ⌈ $5 + 6 = 4$ in $\mathbb{Z}_7$ ⌉ e ⌈ $7 \cdot 7 = 1$ in $\mathbb{Z}_{12}$ ⌉ .

Va tuttavia ricordato che le notazioni più usate sono le tradizionali come ⌈ $a + b \equiv c \pmod{m}$ ⌉ .

B25c.02 Denotiamo a, b e c generiche classi di resti modulo m e abbreviamo $[0]_m$ con 0 e $[1]_m$ con 1.

Prop. Per le operazioni modulari valgono le seguenti proprietà:
(a) $a + b \;=\; b + a$ (commutatività della somma)
(b) $a \cdot b \;=\; b \cdot a$ (commutatività del prodotto)
(c) $(a + b) + c \;=\; a + (b + c)$ (associatività della somma)
(d) $(a \cdot b) \cdot c \;=\; a \cdot (b \cdot c)$ (associatività del prodotto)
(e) $a + 0 = a$ (neutralità verso la somma della classe di 0)
(f) $a \cdot 1 = a$ (neutralità verso il prodotto della classe di 1)
(g) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (distributività del prodotto rispetto alla somma)
(h) Per ogni $a \in \mathbb{Z}_m$ si trova in $\mathbb{Z}$ un solo elemento $-a$ tale che $a + (-a) = 0$ (invertibilità della somma).

Sulle espressioni per le classi di resti si possono quindi effettuare molte manipolazioni formali strettamente simili a quelle per le espressioni riguardanti $\mathbb{Z}$.

Certe manovre però richiedono cautela: la cancellazione di un fattore uguale può non essere lecita: mentre nell'aritmetica ordinaria $a \neq 0$ e $a \cdot b = a \cdot c$ implicano $b = c$, in $\mathbb{Z}_7$ le affermazioni $3 \neq 0$ e $3 \cdot 1 = 3 \cdot 6$ non implicano affatto $1 = 6$.

B25c.03 Presentiamo ora alcune tavole di composizioni per le classi di resti semplificando come già segnalato le scritture $[0]_m,\ [1]_m,\ \ldots\ ,\ [m-1]_m$ nelle 0, 1, ..., $m-1$.

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \qquad \begin{array}{c|ccc} + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array} \qquad \begin{array}{c|ccc} \cdot & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{array}$$

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array} \qquad \begin{array}{c|cccc} \cdot & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 0 & 2 \\ 3 & 0 & 3 & 2 & 1 \end{array} \qquad \begin{array}{c|ccccc} + & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 3 & 4 & 0 \\ 2 & 2 & 3 & 4 & 0 & 1 \\ 3 & 3 & 4 & 0 & 1 & 2 \\ 4 & 4 & 0 & 1 & 2 & 3 \end{array} \qquad \begin{array}{c|ccccc} \cdot & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 \\ 2 & 0 & 2 & 4 & 1 & 3 \\ 3 & 0 & 3 & 1 & 4 & 2 \\ 4 & 0 & 4 & 3 & 2 & 1 \end{array}$$

$$\begin{array}{c|ccccccc} \cdot & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 0 & 2 & 4 & 0 & 2 & 4 \\ 3 & 0 & 3 & 0 & 3 & 0 & 3 \\ 4 & 0 & 4 & 2 & 0 & 4 & 2 \\ 5 & 0 & 5 & 4 & 3 & 2 & 1 \end{array} \qquad \begin{array}{c|ccccccc} \cdot & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 0 & 2 & 4 & 6 & 1 & 3 & 5 \\ 3 & 0 & 3 & 6 & 2 & 5 & 1 & 4 \\ 4 & 0 & 4 & 1 & 5 & 2 & 6 & 3 \\ 5 & 0 & 5 & 3 & 1 & 6 & 4 & 2 \\ 6 & 0 & 6 & 5 & 4 & 3 & 2 & 1 \end{array} \qquad \begin{array}{c|cccccccc} \cdot & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 0 & 2 & 4 & 6 & 0 & 2 & 4 & 6 \\ 3 & 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 \\ 4 & 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\ 5 & 0 & 5 & 2 & 7 & 4 & 1 & 6 & 3 \\ 6 & 0 & 6 & 4 & 2 & 0 & 6 & 4 & 2 \\ 7 & 0 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{array}$$

B25c.04 Osserviamo che tutte le matrici delle somme presentano una unica distribuzione dei valori delle entrate, indipendentemente dal valore di m. Le successive righe presentano successive permutazioni circolari della sequenza $\langle 0, 1, 2, 3, ..., m-1\rangle$. Data la simmetria di queste matrici, equivalente alla commutatività della somma, anche le successive colonne di queste matrici presentano successive permutazioni circolari della suddetta sequenza.

Accenniamo brevemente a un genere di strutture discrete al quale viene dedicato il capitolo D63. Per $m = 2, 3, ...$, si dice **quadrato latino** di ordine m una matrice quadrata avente come codominio un insieme C di m elementi che presenta in ogni riga e in ogni colonna una permutazione di C. Un quadrato latino di ordine 4 e uno di ordine 5 sono

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 4 & 3 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} A & B & C & D & E \\ B & C & A & E & D \\ C & D & E & A & B \\ D & E & B & C & A \\ E & A & D & B & C \end{pmatrix} .$$

Il primo ha codominio $\mathbf{(}4\mathbf{]}$, il secondo $\{A, B, C, D, E\}$, quali che siano i significati che si possono attribuire alle cinque maiuscole.

Per ogni m la tavola di composizione della somma sulle classi di resti modulo m è un quadrato latino relativo al codominio $\mathbf{[}m\mathbf{)}$.

Le tavole per il prodotto sugli $\mathbb{Z}_m$ hanno invece aspetti che dipendono fortemente dal valore di m.
Le matrici relative ai valori primi $m = 2, 3, 5, 7, ...$, eliminando la prima riga e la prima colonna, contenenti solo valori 0 quale che sia m, forniscono quadrati latini di ordine $m-1$ con codominio $\mathbf{(}m\mathbf{)}$.

Anzi tutte le righe e tutte le colonne delle tavole per il prodotto, eccettuate le prime esprimenti la moltiplicazione per 0, presentano permutazioni dell'insieme $\mathbf{(}m\mathbf{)}$.

Si osserva invece che ogni matrice relativa al prodotto su $\mathbb{Z}_m$ con m intero fattorizzabile nelle righe (e nelle colonne) relative a valori v coprimi con m presentano permutazioni di $\mathbf{[}m\mathbf{)}$, mentre nelle righe (e nelle colonne) relative agli altri valori v presentano solo multipli di $\mathrm{MCD}(m, v)$ i quali necessariamente presentano ripetizioni, cioè mettono in evidenza di non fornire quadrati latini.

B25 d. classi di resti invertibili

B25d.01 Una classe di resti $[r]_m \in \mathbb{Z}_m$ è detta **classe di resti invertibile** sse $\mathbb{Z}_m$ contiene qualche s tale che $[r]_m \cdot [s]_m =_m [1]_m$.
In questa situazione la classe $[s]_m$ è detto **elemento inverso** in $\mathbb{Z}_m$ di $[r]_m$ e si scrive $[s]_m = [r]_m^{\mathrm{inv}_m}$ e, se non si rischia l'ambiguità, si scrive $s = r^{\mathrm{inv}_m}$.

Si possono trovare facilmente alcune proprietà degli elementi invertibili di $\mathbb{Z}_m$.

Si vede che, per ogni m $[0]_m$ non è invertibile in $\mathbb{Z}_m$, in quanto $\forall x \in \mathbb{Z}_m : [0]_m \cdot x = [0]_m$.

Un elemento invertibile $[x]_m = x$ possiede un unico elemento inverso; infatti per un tale $r = [r]_m$:

$$\forall x \in \mathbb{Z}_m \quad : \quad r\,x =_m 1\ ,\ rx' =_m 1 \implies x' =_m 1\,x' = (x\,r)x' =_m x(rx') =_m x\ .$$

Per ogni m, l'elemento $[1]_m$ è invertibile in $\mathbb{Z}_m$ e si ha $[1]_m{}^{\mathrm{inv}_m} = [1]_m$.

Anche $m-1 =_m -1$ è invertibile in $\mathbb{Z}_m$ e coincide con il proprio inverso in quanto:
$(m-1)(m-1) = m^2 - 2m + 1 =_m 1$, cioè $(m-1)^{\mathrm{inv}_m} =_m m-1 =_m -1$.

Se r è invertibile in $\mathbb{Z}_m$, cioè se $r \cdot r^{\mathrm{inv}_m} =_m 1$, allora è invertibile anche r^{inv_m}: infatti la precedente uguaglianza equivale alla $(r^{\mathrm{inv}_m})^{\mathrm{inv}_m} =_m r$.

Il passaggio all'inverso in $\mathbb{Z}_m$ è quindi un'involuzione sull'insieme degli elementi invertibili di $\mathbb{Z}_m$.

Inoltre se r e t sono elementi invertibili, lo è anche $r\,t$ e si ha $(r\,t)^{\mathrm{inv}_m} =_m r^{\mathrm{inv}_m}\,t^{\mathrm{inv}_m}$.
Infatti $r\,t\,r^{\mathrm{inv}_m}\,t^{\mathrm{inv}_m} =_m r\,t\,t^{\mathrm{inv}_m}\,r^{\mathrm{inv}_m} =_m r\,r^{\mathrm{inv}_m} =_m 1$.

In molti contesti per l'elemento inverso in $\mathbb{Z}_m$ di una classe di resti r si può abbreviare la notazione r^{inv_m} nella r^{-1}.

B25d.02 Denotiamo con $\mathbf{InvElm}_m(\mathbb{Z}_m)$ l'insieme degli elementi invertibili di $\mathbb{Z}_m$. In questa sezione è lecito abbreviare questa espressione con la più semplice $\mathbf{InvElm}_m$.
Inoltre denotiamo con $\mathbf{InvElmL}(\mathbb{Z}_m)$ o con la sua abbreviazione $\mathbf{InvElmL}_m$ la sequenza degli elementi invertibili di $\mathbb{Z}_m$ presentati in ordine crescente a partire da 1; inoltre useremo le notazioni $k \cdot \mathbf{InvElmL}_m$ per la sequenza dei valori della lista moltiplicati per k modulo m.
Esempi: $\mathbf{InvElmL}_5 = \langle 1,2,3,4\rangle$, $\mathbf{InvElmL}_9 = \langle 1,2,4,5,7,8\rangle$ e $\mathbf{InvElmL}_{12} = \langle 1,5,7,11\rangle$.

Cercando le entrate 1 nelle tabelle dei prodotti in c03 si possono individuare tutti gli elementi invertibili dei $\mathbb{Z}_m$, cioè i sottoinsiemi $\mathbf{InvElm}_m$ dei vari $\mathbb{Z}_m$ per $m = 2,3,...,8$.

Nelle tabelle dei prodotti, oltre alle uguaglianze già acclarate $1^{\mathrm{inv}_m} =_m 1$ e $(m-1)^{\mathrm{inv}_m} =_m 1$, si leggono le seguenti uguaglianze :
$2^{\mathrm{inv}_5} =_5 3$, $2^{\mathrm{inv}_7} =_7 4$, $3^{\mathrm{inv}_7} =_7 5$, $3^{\mathrm{inv}_8} =_8 3$, $5^{\mathrm{inv}_8} =_8 5$.

B25d.03 Nelle formule che seguono con h denotiamo un arbitrario intero naturale maggiore di 1.

(1) Eserc. Dimostrare che per $m = 2h-1$ si ottiene $2^{\mathrm{inv}_m} =_m h$.

(2) Eserc. Più in generale dimostrare che per $m = k\,h - 1$ con k e h interi positivi arbitrari si ha $k^{\mathrm{inv}_m} =_m h$.

(3) Eserc. Fornire attraverso le raffigurazioni cicliche delle congruenze una interpretazione sulla raffigurazione ciclica della formula in (1), e della $3^{\mathrm{inv}_m} =_m h$ per $m = 3\,h - 1$ e della $p^{\mathrm{inv}_m} =_m h$ per $m = p\,h - 1$, ove p denota un arbitrario numero primo.

(4) Eserc. Fornire una interpretazione grafica degli insiemi di multipli, ossia delle righe e colonne della matrice esprimente il prodotto negli insiemi $\mathbb{Z}_m$.

B25d.04 Ricordiamo che due interi positivi k ed n si dicono coprimi sse non presentano fattori comuni, cioè sse $\mathrm{MCD}(k,n)=1$; questa relazione che si presenta anche scrivendo $k \perp n$.

Per ogni n intero positivo denotiamo con $\Phi_{eu}(n)$ il numero di interi appartenenti all'intervallo $\mathbf{(}n\mathbf{)} = \{1,2,...,n-1\}$ che sono coprimi con n; la funzione Φ_{eu} viene chiamata **funzione totient [di Eulero]** e per essa si ha la definizione

$$\Phi_{eu}(n) \;:=\; \big|\{k \in \mathbf{(}n\mathbf{)} \;\big[\!\big]\; k \perp n\}\big| \;\in\; \big\lceil\, \mathbb{P} \longmapsto \mathbb{P} \,\big\rceil \;. \tag{1}$$

I primi valori assunti da questa funzione sono dati dalla seguente tabella funzionale

$$\Phi_{eu} \;=\; \left\downarrow \begin{array}{cccccccccccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & \dots \\ 1 & 1 & 2 & 2 & 4 & 2 & 6 & 4 & 6 & 4 & 10 & 4 & 12 & 6 & 8 & 8 & 16 & 6 & 18 & 8 & \dots \end{array} \right\downarrow .$$

Si osserva subito che se p è un numero primo $\Phi_{eu}(p) = p-1$: infatti la stessa definizione di numero primo dice che tutti gli interi $1,2,...,p-1$ sono coprimi con p.

Si osserva anche che per ogni $k \in \mathbb{P}$ si ha $\Phi_{eu}(2^k) = 2^{k-1}$: infatti sono coprimi con 2^k tutti e solo i dispari inferiori a 2^k.

B25d.05 **(1) Eserc.** Estendere la precedente tabella per la $\Phi_{eu}(n)$ fino a $n=50$.

(2) Eserc. Mostrare che per k e n interi maggiori di 1 e $k<n$ si ha $k \perp n \iff (n-k) \perp n$ e interpretare questa doppia implicazione sulla raffigurazione ciclica come una simmetria di $\mathbf{InvElm}_m$ entro $\mathbf{[}m\mathbf{)}$.

(3) Eserc. Mostrare che, esclusi i casi $m=1,2$, il valore $\Phi_{eu}(m)$ è un intero pari, ossia che

$$\mathsf{cod}(\Phi_{eu}) = \{1\} \cup 2 \cdot \mathbb{P} \;.$$

(4) Eserc. Caratterizzare i poligoni ottenuti dalla raffigurazione ciclica delle classi di $\mathbb{Z}_m$ congiungendo i punti corrispondenti a $\mathbf{InvElm}_m$.

B25d.06 **(1) Prop.**: Un elemento $r \in \mathbb{Z}_m \setminus 0$ è invertibile sse $r \perp m$.

Dim.: "$\Longrightarrow$" Sia $r \in \mathbf{InvElm}_m$ e scriviamo $s := r^{\mathrm{inv}_m}$; si ha $r\,s - 1 = k\,m$ per qualche $k \in \mathbb{P}$; ma $\mathrm{MCD}(r,m) \,|\, r\,s$ e $\mathrm{MCD}(r,m) \,|\, k\,m$ e quindi $\mathrm{MCD}(r,m) \,|\, r\,s - k\,m$, ergo $\mathrm{MCD}(r,m) = 1$, i.e. $r \perp m$ ∎

"$\Longleftarrow$" Sia $r \perp m$, i.e. $\mathrm{MCD}(r,m)=1$; mediante l'algoritmo euclideo si trovano interi a e b tali che $r\,a + m\,b = 1$; ergo $r\,a - 1 =_m 0$, i.e. $r \in \mathbf{InvElm}_m$ ∎

(2) Coroll.: Se p è un numero primo, allora $\mathbf{InvElm}_p = \mathbf{(}p\mathbf{)}$.

B25d.07 **(1) Prop.**: La moltiplicazione modulo m per qualsiasi elemento di $\mathbf{InvElm}_m$ e il passaggio all'inverso in $\mathbb{Z}_m$ entro $\mathbf{InvElm}_m$ sono permutazioni; il passaggio all'inverso è più precisamente una involuzione.

Dim.: Sia $t \in \mathbf{InvElm}_m$ e consideriamo la sequenza $t \cdot \mathbf{InvElmL}_m$. Dato che per ogni $s \in \mathbf{InvElm}_m$ è $t\,s \in \mathbf{InvElm}_m$, si ha $t \cdot \mathbf{InvElm}_m \subseteq \mathbf{InvElm}_m$.
Viceversa $t \cdot \mathbf{InvElm}_m \subseteq \mathbf{InvElm}_m$, in quanto a ogni $s \in \mathbf{InvElm}_m$ si può dare la forma $s = t(t^{\mathrm{inv}_m} s)$. Per la precisazione sulla involuzione basta ricordare che ogni passaggio all'elemento inverso è una involuzione ∎

Esempi: $3 \cdot \mathbf{InvElmL}_5 = \langle 3,1,4,2\rangle$ e $7 \cdot \mathbf{InvElmL}_{12} = \langle 7,11,1,5\rangle$.

B25d.08 **Teorema** (**teorema di Eulero**)
$\forall r \in \mathbf{InvElm}_m \;:\; r^{\Phi_{eu}(m)} =_m 1$.

Dim.: Scriviamo $\phi := \Phi_{eu}(m)$ e $\{s_1, s_2, ..., s_\phi\} := \mathbf{InvElm}_m$; poniamo inoltre $t :=_m s_1 s_2 \cdots s_\phi$. Per la proposizione precedente, per il generico $r \in \mathbf{InvElm}_m$ si ha $t =_m (rs_1)(rs_2)\cdots(rs_\phi) = r^\phi t$; inoltre, essendo t invertibile, $1 =_m t\, t^{\mathrm{inv}_m} =_m r^\phi$ ∎

B25**d.09** **Coroll.**: (**piccolo teorema di Fermat**) Se p è un numero primo e $t \in \mathbb{P} \setminus p \cdot \mathbb{P}$, cioè se t è un intero positivo coprimo con p, allora $t^{p-1} =_p 1$.

Dim.: Discende subito dal precedente, in quanto t è invertibile in $\mathbb{Z}_p$ e $\Phi_{eu}(p) = p - 1$ ∎

B25**d.10** La d07(1) implica che riducendo la tavola di moltiplicazione di $\mathbb{Z}_m$ alla sottomatrice riguardante solo gli elementi di $\mathbf{InvElm}_m$ si ottiene un quadrato latino [D63], cioè una matrice che in ciascuna riga e in ciascuna colonna presenta una permutazione di elementi di $\mathbf{InvElm}_m$.

Per esempio le matrici per i casi $m = 2, 3, 4, 5$ ed $m = 6, 7, 8$ si riducono ai seguenti quadrati latini.

$$\begin{array}{c|c} & 1 \\ \hline 1 & 1 \end{array} \qquad \begin{array}{c|cc} & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 1 \end{array} \qquad \begin{array}{c|cc} & 1 & 3 \\ \hline 1 & 1 & 3 \\ 3 & 3 & 1 \end{array} \qquad \begin{array}{c|cccc} \cdot & 1 & 2 & 3 & 4 \\ \hline 1 & 1 & 2 & 3 & 4 \\ 2 & 2 & 4 & 1 & 3 \\ 3 & 3 & 1 & 4 & 2 \\ 4 & 4 & 3 & 2 & 1 \end{array}$$

$$\begin{array}{c|cc} & 1 & 5 \\ \hline 1 & 1 & 5 \\ 5 & 5 & 1 \end{array} \qquad \begin{array}{c|cccccc} \cdot & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 2 & 4 & 6 & 1 & 3 & 5 \\ 3 & 3 & 6 & 2 & 5 & 1 & 4 \\ 4 & 4 & 1 & 5 & 2 & 6 & 3 \\ 5 & 5 & 3 & 1 & 6 & 4 & 2 \\ 6 & 6 & 5 & 4 & 3 & 2 & 1 \end{array} \qquad \begin{array}{c|cccc} \cdot & 1 & 3 & 5 & 7 \\ \hline 1 & 1 & 3 & 5 & 7 \\ 3 & 3 & 1 & 7 & 5 \\ 5 & 5 & 7 & 1 & 3 \\ 7 & 7 & 5 & 3 & 1 \end{array}$$

(d.11) Eserc. Costruire le matrici di moltiplicazione per gli elementi degli $\mathbf{InvElm}_m$ per $m = 9, 10, 11, 12, 13$.

B25 e. coppie e terne pitagoriche

B25e.01 Definiamo preliminarmente la notazione per l'insieme dei quadrati dei numeri naturali

$$\mathbb{N}_{sq} \;:=\; \{n \in \mathbb{N} :|\; n^2\}\ .$$

Definiamo quindi **coppia pitagorica.g** ogni coppia di interi $\langle a, b\rangle \in \mathbb{Z} \times \mathbb{Z}$ tali che $a^2 + b^2$ sia il quadrato di un intero positivo, ovvero tali che sia $a^2 + b^2 \in \mathbb{N}_{sq}$.

Una coppia pitagorica.g si dice coppia pitagorica.g impropria sse $a = 0$ oppure $b = 0$, mentre si dice coppia pitagorica.g propria ogni coppia con le due componenti nonnulle. Tra le coppie improprie si trova $\langle 0, 0\rangle$ detta coppia pitagorica nulla.

Chiaramente l'insieme delle coppie pitagoriche.g improprie è dato da

$$\bigcup_{q\in\mathbb{N}_{sq}} \{\langle q, 0\rangle, \langle -q, 0\rangle, \langle 0, q\rangle, \langle 0, -q\rangle\}\ \ ,$$

cioè dai punti-ZZ appartenenti agli assi e aventi coordinate che in valore assoluto sono quadrati di interi. Queste coppie presentano scarso interesse costruttivo, ma consentono di semplificare alcuni enunciati.

Si osserva che nessuna coppia pitagorica.g presenta le due componenti uguali, in quanto nessun intero della forma $2\,a^2$ può essere il quadrato di un intero, ovvero

$$2 \cdot \mathbb{N}_{sq} \cap \mathbb{N}_{sq} \;=\; \{\langle 0, 0\rangle\}\ .$$

Volendo generalizzare abbiamo $\;(\mathbb{N} \setminus \mathbb{N}_{sq}) \cap \mathbb{N}_{sq} \;=\; \{\langle 0, 0\rangle\}\ .$

Si osserva che le riflessioni-ZZ rispetto agli assi e rispetto alla diagonale principale e alla secondaria trasformano una coppia pitagorica.g in una coppia pitagorica.g ottenuta cambiando di segno a qualcuna delle omponenti e/o scambiandole.
Più in dettaglio: la riflessione-ZZ rispetto Oy cambia di segno alla prima componente, la riflessione rispetto ad Ox cambia il segno della seconda coponente, la riflessione rispetto alla diagonale principale scambia le due componenti e la riflessione rispetto alla codiagonale scambia le componenti e cambia i loro segni.

Ad ogni coppia pitagorica.g propria $\langle a, b\rangle$ si associa la cosiddetta terna pitagorica.g

$$\big\langle\, \min(|a|, |b|)\ ,\ \max(|a|, |b|)\ ,\ c\big\rangle\ ,$$

dove c è l'intero positivo tale che $a^2 + b^2 = c^2$.
Si constata che applicando a una coppia pitagorica.g propria una riflessione rispetto a un asse o rispetto a una diagonale non si cambia la corrispondente terna pitagorica. Di conseguenza si può limitare lo studio alle coppie pitagoriche.g costituite da due interi positivi il primo minore del secondo.
Queste le chiamiamo *tout court* **coppie pitagoriche** e le corrispondenti terne pitagoriche.g le chiamiamo **terne pitagoriche**.

Evidentemente la corripondenza biunivoca tra coppie pitagoriche.g e terne pitagoriche.g comprende come sottoinsieme la corrispondenza biunivoca tra coppie pitagoriche e terne pitagoriche.

Va segnalato che le prime terne pitagoriche documentate compaiono in una tavola cuneiforme babilonese scritta intorno al 1800 a.C. e quindi sarebbe più corretto chiamarle "terne babilonesi-pitagoriche".

B25e.02 Evidentemente se $\langle a, b\rangle$ è una coppia pitagorica per ogni $k \in \mathbb{P}$ lo è anche $\langle k\,a, k\,b$.

Quindi le coppie pitagoriche che presentano maggior interesse sono quelle costituite da due interi positivi coprimi, il primo inferiore al secondo. Queste sono dette **coppie pitagoriche primitive** e le corrispondenti terne sono dette **terne pitagoriche primitive**.

Sono terne pitagoriche primitive $\langle 3,4,5\rangle$, $\langle 5,12,13\rangle$ e $\langle 7,24,25\rangle$; sono invece terne pitagoriche non primitive $\langle 6,8,10\rangle$, $\langle 15,36,39\rangle$ e $\langle 42,144,150\rangle$.

Eserc. (1) Verificare che tutte le terne $\big\langle 2d+1\ ,\ 2d(d+1)\ ,\ 2d(d+1)+1\big\rangle$ per $d=2,3,...$ sono terne pitagoriche primitive.

Il fatto precedente comporta che esistono infinite coppie pitagoriche primitive e infinite terne pitagoriche primitive.

Si osserva che sono terne pitagoriche primitive anche $\langle 8,15,17\rangle$, $\langle 12,35,37\rangle$, $\langle 20,21,29\rangle$ e $\langle 20,99,101\rangle$.

Eserc. (2) Dimostrare che non esistono terne pitagoriche primitive $\langle a,b,c\rangle$ con $a+b$ pari e quindi che le terne pitagoriche primitive aut hanno la prima componente pari e la seconda e la terza dispari, aut hanno la prima componente dispari, la seconda pari e la terza dispari.

B25e.03 **Prop.** Consideriamo una coppia di interi $\langle m,n\rangle$ con $m>n>1$. Chiamiamo **espressioni generatrici di Euclide** le espressioni

$$a := m^2-n^2 \quad , \quad b := 2\,m\,n \quad , \quad c := m^2+n^2\ . \tag{1}$$

(2) Prop.: (a) La terna $\langle a,b,c\rangle$ è una terna pitagorica.
(b) Questa terna è primitiva sse $m\perp n$ ed m ed n non sono entrambi dispari.
(c) Tutte le terne pitagoriche primitive $\langle a,b,c\rangle$ sono fornite dalle tre espressioni generatrici di Euclide.

Dim.: (a) $a^2+b^2 \;=\; (m^2-n^2)^2+(2mn)^2 \;=\; (m^2+n^2)^2 \;=\; c^2$.

(b) Si osserva che se un primo p dividesse due dei tre membri di una terna primitiva dovrebbe dividere anche il terzo e quindi la terna non sarebbe primitiva.
Supponiamo che sia a sia dispari e quindi b sia pari e c dispari; (se a fosse pari e b dispari si avrebbero conseguenze equivalenti).

$$a^2+b^2 \;=\; c^2 \iff (c-a)(c+a) \;=\; b^2 \iff \frac{c+a}{b} \;=\; \frac{b}{c-a}\ .$$

Essendo $\dfrac{c+a}{b}$ razionale si può riscrivere come $\dfrac{m}{n}$ con $m\perp n$ e si ha $\dfrac{c-a}{b} \;=\; \dfrac{n}{m}$. Abbiamo quindi

$$\frac{c}{b}+\frac{a}{b}=\frac{m}{n} \quad \text{e} \quad \frac{c}{b}-\frac{a}{b}=\frac{n}{m}\ ;$$

Consideriamo questo un sistema di due equazioni lineari in $\frac{c}{b}$ e $\frac{a}{b}$ si ottiene

$$\frac{c}{b} \;=\; \frac{1}{2}\Big(\frac{m}{n}+\frac{n}{m}\Big) \;=\; \frac{m^2+n^2}{2mn} \qquad , \qquad \frac{a}{b} \;=\; \frac{1}{2}\Big(\frac{m}{n}-\frac{n}{m}\Big) \;=\; \frac{m^2-n^2}{2mn}\ .$$

Dato che $m\perp n$ non possono essere entrambi interi pari. Se fossero entrambi dispari m^2-n^2 con $m=2\mu+1$ en $n=2\nu+1$ si avrebbe $m^2-n^2=4\nu^2+4\nu-4\mu^2-4\mu$ cioè sarebbe multiplo di 4, mentre sarebbe $2mn \;=_2\; 2$ e quindi a/b non sarebbe intero.
Si deve avere uno dei due interi m e n pari e l'altro dispari e quindi anche in questi casi sarebbe $2mn \;=_2\; 2$. I due numeratori sono dispari e il denominatore è pari. Quindi le espressioni trovate implicano che devono essere uguali i numeratori e devono essere uguali i denominatori. Di conseguenza:

$$a=m^2-n^2 \quad , \quad b=2mn \quad , \quad c=m^2+n^2 \quad , \quad m\perp n \quad , \quad m+n=_2 1 \ \blacksquare$$

B25e.04 Le espressioni generatrici di Euclide forniscono biunivocamente tutte le terne pitagoriche primitive, ma non forniscono le non primitive, per esempio non forniscono la semplice terna $\langle 9, 12, 15\rangle$, multiplo triplo della primitiva $\langle 3, 4, 5\rangle$.

Una formula in grado di fornire tutte le terne pitagoriche si ottiene dalle e03(1) facendo intervenire un terzo parametro k.

(1) Prop.: Tutte le terne pitagoriche sono fornite biunivocamente dalle espressioni

$$a = k \cdot (m^2 - n^2)\ ,\ b = k \cdot 2mn\ ,\ c = k \cdot (m^2 + n^2)$$
$$\text{per} \quad k \in \mathbb{P}\ ,\ n = 2, 3, 4, ...\ \text{ ed }\ m = n+1, n+2, ...$$

Una variante delle tre espressioni di Euclide per le terne primitive che in qualche circostanza è più conveniente è indicata dal seguente enunciato.

(2) Prop.: Se m ed n sono interi dispari tali che $m > n > 1$, allora ogni $\langle a, b, c\rangle$ con $a = mn$, $b = \dfrac{m^2 - n^2}{2}$ e $c = \dfrac{m^+n^2}{2}$ fornisce una terna pitagorica con a dispari e b pari e ogni $\langle a, b, c\rangle$ con $a = \dfrac{m^2 - n^2}{2}$, $b = mn$ e $c = \dfrac{m^+n^2}{2}$ fornisce una terna pitagorica con a pari e b dispari; una tale terna è primitiva sse $m \perp n$.

Inoltre ogni tripla pitagorica primitiva è ottenibile da uno solo dei due gruppi di formule precedenti con $m > n > 1$ interi dispari e coprimi.

B25 f. somme di divisori

B25f.01 Introduciamo la **funzione somma dei divisori** che a ogni intero positivo m associa la somma dei suoi divisori (1 ed m compresi):

$$\mathsf{Sdvsr} \;:=\; \left\lceil\, m \in \mathbb{P} \mapsto \sum_{j \preceq_: m} j \,\right\rceil \;. \tag{1}$$

Nei testi della teoria dei numeri questa funzione viene solitamente denotata con $\sigma(n)$.

Si tratta di una funzione del genere $\lceil\, \mathbb{P} \longmapsto \mathbb{P} \,\rceil$ facilmente valutabile per ogni m per il quale si sia individuato l'insieme dei divisori.

La rappresentazione tabellare di una prima parte di questa funzione è la seguente

$$\mathsf{Sdvsr} \;=\; \left\downarrow \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & ... \\ 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 & 12 & 28 & 14 & 24 & 24 & 31 & 18 & 39 & 20 & 42 & ... \end{matrix} \right\downarrow$$

Come si può constatare la funzione Sdvsr non è monotona e non è invertibile.

B25f.02 Le prime proprietà della funzione Sdvsr si osservano facilmente.

(1) Prop.: Se p è primo, allora $\mathsf{Sdvsr}(p) = p + 1$ ∎

(2) Prop.: Se r è maggiore di 1 e non è primo, allora $\mathsf{Sdvsr}(r) > p + 1$ ∎

(3) Prop.: $\forall k \in \mathbb{P} \;:\; \mathsf{Sdvsr}(2^k) = 2^{k+1} - 1$ ∎

(4) Prop.: Per ogni p numero primo e per ogni $k \in \mathbb{P}$ si ha $\mathsf{Sdvsr}(p^k) \;=\; \dfrac{p^{k+1} - 1}{p - 1}$.

Dim.: Basta osservare che $\mathsf{Dvsr}(p^k) = \{1, p, p^2, p^3, ..., p^k\}$ e che

$$\forall n \in \mathbb{P}, b \in \mathbb{P} \;:\; \left(\textstyle\sum_{i=0}^{n} b^i\right)(b-1) \;=\; h^{n+1} - 1$$ ∎

(5) Prop.: Per ogni $m = 2, 3, 4, ...$ valgono le disuguaglianze $m + 1 \leq \mathsf{Sdvsr}(m) \leq \dfrac{m(m+1)}{2}$ ∎

Si può quindi affermare che la funzione Sdvsr, oltre a non essere monotona e non essere invertibile, non è limitata superiormente e in media va crescendo almeno linearmente.
Si vede che tutti i valori associati agli interi compresi tra due primi successivi p e q sono maggiori di $q + 1 = \mathsf{Sdvsr}(q)$. Quindi questa funzione ha un andamento con minimi locali con valori che crescono linearmente, ovvero con valori che si mantengono superiori a quelli della funzione $\lceil\, n \mapsto n \,\rceil$.

Si può anche dire che il suo maggiore valore è un significativo indicatore di una maggiore divisibilità.

B25f.03 Una importante proprietà della funzione Sdvsr è la seguente.

(1) Prop.: Se $m_1, m_2 \in \mathbb{P}$ con $m_1 \perp m_2$, allora $\mathsf{Sdvsr}(m_1 \cdot m_2) \;=\; \mathsf{Sdvsr}(m_1) \cdot \mathsf{Sdvsr}(m_2)$.

Dim.: Sia Nel prodotto cartesiano $\{2, 3, ...\} \times \mathbb{N}$ si possono osservare i due istogrammi dei divisori di m_1 e di m_2.
Sia d un intero positivo che divide $m_1 \cdot m_2$; a un tale intero positivo si può associare una coppia $\langle d_1, d_2 \rangle \;\in\; \mathsf{Dvsr}(m_1) \times \mathsf{Dvsr}(m_2)$, tale che $d_1 \preceq_: m_1$ e $d_2 \preceq_: m_2$, e quindi una coppia di fattorizzazioni riguardanti, risp., d_1 e d_2.
Dunque si hanno le uguaglianze

$$\begin{aligned} \mathsf{Sdvsr}(m_1 \cdot m_2) \;&=\; \sum_{d \preceq_: m_1 \cdot m_2} d \;=\; \sum_{d_1 \preceq_: m_1 \;,\; d_2 \preceq_: m_2} d_1 \cdot d_2 \;=\; \left(\sum_{d_1 \preceq_: m_1} d_1\right) \cdot \left(\sum_{d_2 \preceq_: m_2} d_2\right) \\ &=\; \mathsf{Sdvsr}(m_1) \cdot \mathsf{Sdvsr}(m_2) \end{aligned}$$ ∎

La proposizione precedente si generalizza senza difficoltà.

(2) Prop.: Se per $h = 2, 3, 4, ...$ abbiamo h interi positivi $m_1, ..., m_h$ a due a due coprimi, allora

$$\mathsf{Sdvsr}\left(\prod_{j=1,...,h} m_j\right) \;=\; \prod_{j=1,...,h} \mathsf{Sdvsr}(m_j)\,.$$

Per ogni intero m maggiore o uguale a 2 la fattorizzazione nelle successive potenze di numeri primi divisori consente di ottenere per la somma dei suoi divisori un'espressione dall'aspetto algebrico .

(3) Prop.: Di un intero $m \in \{2, 3, ...\}$ si conosca la fattorizzazione mediante numeri primi

$$m \;=\; {p_{<1>}}^{e_1}\, {p_{<2>}}^{e_2} \,...\, {p_{<h>}}^{e_h} \quad , \text{ con } e_1, e_2, ..., e_h \text{ interi positivi.}$$

Allora si ha $\mathsf{Sdvsr}(m) \;=\; \dfrac{{p_{<1>}}^{e_1+1}-1}{p_{<1>}-1} \cdot \dfrac{{p_{<2>}}^{e_2+1}-1}{p_{<2>}-1} \cdots \dfrac{{p_h}^{e_{<h>}+1}-1}{p_{<h>}-1}$.

Dim.: Basta applicare la f02(4) e la f02(2) ∎

B25 g. numeri perfetti e numeri amicabili

B25g.01 Della funzione $\mathsf{Sdvsr}(m)$ interessano anche le due varianti che seguono.
Si dice **funzione somma dei divisori propri** la funzione del genere $\lceil\!\lceil\, \mathbb{P} \longmapsto \mathbb{P} \,\rceil\!\rceil$

$$\mathsf{Sdvsrp} \;:=\; \lceil\!\lceil\, m \in \mathbb{P} \;\mapsto\; \mathsf{Sdvsr}(m) - m \,\rceil\!\rceil \;=\; \lceil\!\lceil\, m \in \mathbb{P} \;\mapsto\; \sum_{j \prec_! m} j \,\rceil\!\rceil \;. \tag{1}$$

È interessante anche l'andamento della funzione

$$\lceil\!\lceil\, m \in \mathbb{P} \;\mapsto\; \mathsf{Sdvsr}(m) - 2\,m \,\rceil\!\rceil \;.$$

Si tratta di una funzione del genere $\lceil\!\lceil\, \mathbb{P} \longmapsto \mathbb{Z} \,\rceil\!\rceil$ che presenta valori negativi (ad esempio vale $-(p-1)$ per ogni numero primo p), valori nulli e valori positivi.
Gli interi positivi m per i quali $\mathsf{Sdvsr}(m) - m < 0$ si dicono **numeri deficienti**, quelli $\mathsf{Sdvsr}(m) - m > 0$ si dicono **numeri abbondanti** e quelli con $\mathsf{Sdvsr}(m) = m$, ad esempio 6, sono detti **numeri perfetti**.

Denotiamo con $\mathbb{P}_{perf}$ l'insieme dei numeri perfetti.

B25g.02 Chiamiamo **coppia di numeri amicabili** (talvolta chiamati "numeri amici") ogni coppia di interi positivi m ed n con $m \le n$ tali che $\mathsf{Sdvsrp}(m) = n$ e $\mathsf{Sdvsrp}(n) = m$.
Come si constata senza difficoltà un esempio di tale coppia è la $\langle 220, 284 \rangle$.
Denotiamo con AmcbC l'insieme delle coppie di numeri amicabili.

I numeri amicabili sono conosciuti fin dal tempo dei pitagorici e sono stati ampiamente studiati. Presso i greci e per la Bibbia a queste coppie era attribuito il valore nmagico di propiziatori di amicizia e amore.

Una coppia di numeri amicabili, $\langle 17\,296 \;,\; 18\,416 \rangle$ fu scoperta nel XIII secolo dall'arabo al-Banna e riscoperta nel 1636 da Fermat; La coppia $\langle 9\,363\,584 \;,\; 9\,437\,056 \rangle$ fu scoperta da Descartes.

Nel IX secolo il matematico arabo Thabit ibn Qurra trovò una formula in grado di esprimere alcune decine di coppie di numeri amicabili.
Per ogni intero positivo Q che rende primi i numeri

$$a := 3\,2^Q - 1 \quad , \quad b := 3\,2^{Q-1} - 1 \quad \text{e} \quad c := 9\,2^{2Q-1} - 1 \;,$$

abbiamo che

$$\langle 2\,Q\,a\,b \;,\; 2\,n\,c \rangle \text{ è una coppia amicabile .}$$

Intorno al 1750 Euler generalizzò questa formula e riuscì a esprimere 62 coppie di numei amicabili.
[`http://www.bitman.name/math/article/59`] Fiorentini Amichevoli (numeri)] (I)

Se $p = 2m(2n - m + 1) - 1$, $q = 2n(2n - m + 1) - 1$ e $r = 2n + m(2n - m + 1)2 - 1$ sono numeri primi con $4n > m > 0$, allora $2npq$ e $2nr$ formano una coppia di numeri amicabili.

Nel secolo XIX si conoscevano una sessantina di coppie amicabili; da notare che la seconda più piccola, $\langle 1184 \;,\; 1210 \rangle$, fu scoperta nel 1867 da un sedicenne Nicolò Paganini, omonimo del celebre violinista.

Sono state proposte altre formule in grado di esprimere coppie di numeri amicabili, ma nessuna fornisce tutte le coppie note.

Nel 1946 erano note 390 coppie di numeri amicabili e successivamente sono stati oggetto di indagini esaustive mediante il computer e attualmente si conoscono oltre un miliardo e 200 milioni di coppie.
Altre coppie sono

$\langle 2620, 2924\rangle$, $\langle 5020, 5564\rangle$, $\langle 6232, 6368\rangle$, $\langle 10\,744, 10\,856\rangle$, $\langle 17\,296, 18\,416\rangle$, $\langle 63\,020, 76\,084\rangle$, $\langle 66\,92866\,992\rangle$, $\langle 67\,095, 71\,145\rangle$, $\langle 69\,615, 87\,633\rangle$, $\langle 122\,265, 153\,176\rangle$, $\langle 141\,664, 153\,176\rangle$, $\langle 142\,310, 168\,730\rangle$, $\langle 171\,856, 176\,336\rangle$, $\langle 176\,272, 180\,848\rangle$, $\langle 196\,724, 202\,444\rangle$, $\langle 308\,620, 389\,924\rangle$, $\langle 437\,456, 455\,344\rangle$, $\langle 503\,056, 514\,736\rangle$, $\langle 522\,405, 525\,915\rangle$, $\langle 609\,928, 686\,072\rangle$, $\langle 1\,175\,265, 1\,438\,983\rangle$, $\langle 1\,280\,565, 1\,340\,235\rangle$, $\langle 1\,358\,595, 1\,486\,845\rangle$, $\langle 9\,363\,584, 9\,437\,056\rangle$, $\langle 196\,421\,715, 224\,703\,405\rangle$.

Le coppie costituite da due repliche dello stesso numero perfetto sono assimilabili alle coppie di numeri amicabili e spesso sono inserite nell'insieme AmcbC.

Tutte le coppie di numeri amicabili sono costituite da numeri entrambi pari o entrambi dispari e non si sa se ne esistano di interi di parità diverse.
Non si sa neppure se l'insieme delle coppie sia finito o infinito.
Sono note coppie amicabili diverse ma con una componente in comune.

Altre informazioni sui numeri amicabili e varie altre categorie di numeri interi si trovano in `www.bitman.name/math/`.

B25g.03 Si dice **coppia di numeri fidanzati** o di "numeri quasiamicabili"ogni coppia di numeri interi positivi per i quali la somma dei divisori propri e maggiori di 1 di un componente è uguale all'altro e viceversa.
Una tale coppia è per esempio formata dai numeri 48 e 75.
Infatti: $2 + 3 + 4 + 6 + 8 + 12 + 16 + 24 = 75$, mentre $3 + 5 + 15 + 25 = 48$.

Altre coppie di fidanzati sono $\langle 140, 195\rangle$ e $\langle 1\,575, 1\,648\rangle$; La coppia più grande oggi nota è $\langle 2\,102\,750, 2\,681\,019\rangle$.

Diciamo ricerca della felicità di un numero in notazione decimale la sua trasformazione nella somma dei quadrati delle sue cifre. Si dice **numero felice** un intero positivo se applicandogli la ricerca della felicità e ripetendo l'operazione ai numeri successivamente ottenuti si giunge al numero 1.

Un numero felice è 19, in quanto 1+81=82; 64+4=68; 36+64=100; 1+0+0=1; evidentemente sono felici anche 82, 68, 100; ed anche 190, 8 200, $68 \cdot 100^5$ e, mi voglio rovinare, tutte le potenze di 10.

Si dice **ciclo di numeri socievoli** una sequenza ciclica di interi positivi $\langle_{cy} s_1, s_2, ..., s_k = s_0\rangle$ con $k = 3, 4, ...$ tale che per ogni $h = 0, 1, 2, ..., k-1$ si ha $\mathsf{Sdvsrp}(s_h) = s_{h+1}$.

Un esempio di tale ciclo è dato da $\langle_{cy} 12\,496, 14\,288, 15\,472, 14\,536, 14\,264\rangle$.

B25g.04 I primi numeri perfetti sono:

6 28 496 8 128 33 550 336 8 589 869 056 137 438 691 328
2 305 843 008 139 952 128 2 658 455 991 569 831 744 654 692 615 953 842 176 .

L'esposizione in https://www.mi.imati.cnr.it/alberto/ e https://arm.mi.imati.cnr.it/Matexp/matexp_main.php