CAPITOLO 2
LE STRUTTURE ALGEBRICHE

2.1 Strutture algebriche. Gruppi

Abbiamo visto che sull'insieme dei numeri naturali si può fare molto più delle semplici operazioni aritmetiche. Introduciamo alcuni concetti fondamentali per uno studio più approfondito di un insieme numerico.

Definiamo **interna** un'operazione tra elementi di un insieme A, che si dice **chiuso**, se il risultato dell'operazione è ancora un elemento dell'insieme.

La coppia costituita dall'insieme A e dall'operazione binaria interna *, che indichiamo con $(A,*)$, si dice **struttura algebrica**. Vediamo qualche esempio.

L'insieme dei numeri naturali è chiuso rispetto all'addizione, ma non lo è rispetto alla sottrazione.

Più interessante è l'insieme dei numeri *interi* Z, all'interno del quale valgono le seguenti proprietà:

1. Se $x, y \in Z \Rightarrow x + y = z \in Z$ (**chiusura**);
2. Se $x, y, z \in Z \Rightarrow (x + y) + z = x + (y + z)$ (**associatività**);
3. $\forall x \in Z$ si ha che $x + 0 = 0 + x = x$ (**elemento neutro** 0);
4. $\forall x \in Z, \exists \overline{x} \in Z \mid x + \overline{x} = \overline{x} + x = 0$ (**opposto** di *x*).

In generale, se un insieme A viene munito di un'operazione binaria interna, rispetto alla quale valgono le proprietà 1-4 di cui sopra, l'insieme si dice **gruppo**. I gruppi sono quindi delle particolari strutture algebriche.

Esercizio. L'insieme dei numeri naturali, escluso lo zero, munito dell'operazione che associa ad ogni coppia di numeri naturali il loro massimo comun divisore, è un gruppo?

2.2 Classi di resto

Consideriamo, all'interno dell'insieme dei numeri interi, la relazione che associa due numeri *a*, *b* se questi danno lo stesso resto nella divisione per uno stesso numero *n*. Una relazione di questo tipo si dice **congruenza**, ed i numeri *a*, *b* si dicono **congrui modulo *n***. Con la notazione di Gauss si scrive:

$$a \equiv b \bmod(n),$$

che si legge "a è congruo a b modulo n", se $n \mid (a - b)$.

La congruenza modulo *n* è una **relazione di equivalenza** sull'insieme dei numeri interi. Verifichiamo le proprietà.

1. Proprietà **riflessiva**: $n \mid 0 = a - a \Rightarrow a \equiv a \bmod(n)$;
2. Proprietà **simmetrica**: $n \mid (a - b) \Rightarrow n \mid -(a - b) = (b - a) \Rightarrow b \equiv a \bmod(n)$;
3. Proprietà **transitiva**: $n \mid (a - b)$, $n \mid (b - c) \Rightarrow n \mid (a - b + b - c) \Rightarrow a \equiv c \bmod(n)$.

Le relazioni di equivalenza operano una **partizione** nell'insieme in cui sono definite, suddividendolo cioè in sottoinsiemi, detti **classi di equivalenza**, tali che:

I. L'unione di tutti i sottoinsiemi forma l'insieme di partenza;
II. L'intersezione di due qualsiasi sottoinsiemi distinti è l'insieme vuoto;
III. Nessun sottoinsieme è vuoto.

L'insieme degli interi, con la relazione di congruenza, viene suddiviso in classi di equivalenza dette **classi di resto**. L'insieme formato dalle classi di equivalenza è detto **insieme quoziente**.

In particolare, si denota con $Z_n \equiv \{[0],[1],...,[n-1]\}$ l'insieme quoziente degli interi in base alla relazione di congruenza modulo *n*. Le classi di resto $[j]$, con $j = 0,1,2...,n-1$ contengono ognuna gli interi che, nella divisione per *n*, danno come resto *j*.

Anche sull'insieme Z_n è possibile definire un'operazione binaria interna, che lo rende una struttura algebrica. In particolare, la struttura algebrica $(Z_n,+)$ è un gruppo. Verifichiamo gli assiomi 1-4, osservando che $x\in[j]\Rightarrow x=kn+j$, $k\in Z$.

1. (*chiusura*): $[i]+[j]=\begin{cases}[i+j]; & i+j\le n-1\\ [i+j-n]; & i+j\ge n\end{cases}$;
2. (*associatività*): $([i]+[j])+[k]=[i]+([j]+[k])$;
3. (*opposto*): $\forall[i]\in Z_n,\exists -[i]=[n-i]\,|\,[i]+[n-i]=[0]$;
4. (*elemento neutro*): è la classe di resto $[0]$.

Il gruppo $(Z_n,+)$ è tale che l'operazione è commutativa: $[i]+[j]=[j]+[i]$. I gruppi che hanno questa proprietà si dicono **abeliani**.
Il comportamento delle classi di resto rispetto all'operazione di addizione può essere riassunto nelle cosiddette **tavole di composizione**. Vediamo come si costruiscono.

$(Z_4,+)$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Una lettura attenta della tavola di composizione permette di ritrovare gli assiomi della struttura di gruppo (e, in particolare, verificare agevolmente l'associatività).
Consideriamo le seguenti proprietà "aggiuntive" della congruenza: se $a\equiv a'\bmod(n)$ e $b\equiv b'\bmod(n)$, allora

4. $(a\pm b)\equiv(a'\pm b')\bmod(n)$;
5. $ab\equiv a'b'\bmod(n)$.

Esercizio. Porre $a=a'+rn$ e $b=b'+sn$ e verificare le proprietà 4 e 5 della congruenza.

Le equazioni con le classi di resto
Un'interessante applicazione del metodo per la ricerca delle soluzioni intere di un'equazione diofantea, è rappresentata dal procedimento per la risoluzione delle equazioni con le classi di resto, ovvero equazioni del tipo

$$[ax]=[b]\bmod(n).$$

Intanto, qual è il significato di questa scrittura? Dire $[ax]=[b]$ modulo *n* significa affermare che le due classi di resto coincidono, e se due numeri appartengono alla stessa classe di resto, allora sono congrui modulo *n*, quindi *n* divide la loro differenza:

$$ax-b=ny.$$

Di conseguenza, risolvere l'equazione $[ax]=[b]\bmod(n)$ equivale a cercare le soluzioni intere in *x* (che ci interessa) ed in *y* (che ci interessa meno), dell'equazione $ax-ny=b$.
Esempio. Risolvere l'equazione $[14x]=[21]\bmod(77)$.

- In base a quanto appena accennato cerchiamo le soluzioni intere dell'equazione $14x-77y=21$. Possiamo dividere ambo i membri per 7, ottenendo l'equazione equivalente $2x-11y=3$. Verificato che quest'equazione ammette soluzioni intere, il metodo per la loro

ricerca conduce alle soluzioni $\begin{cases} x = 11n - 15 \\ y = 2n - 3 \end{cases}$. A noi interessa $x = 11n - 15$. Ora, poiché $15 = 11 + 4$, la soluzione può essere scritta in una forma più adeguata al contesto in cui è inserita, ovvero quello delle classi di resto: $x = 11n - 4$.

2.3 Il binomio di Newton e la divisibilità

Per "binomio di Newton" si intende un'espressione del tipo $(a+b)^n$. Lo sviluppo di questo binomio può essere associato al cosiddetto "triangolo di Tartaglia", con il quale vengono rappresentati (a meno del segno) i coefficienti dello sviluppo:

1

1 2 1 $\Rightarrow (x+y)^2 = x^2 + 2xy + y^2$

1 3 3 1 $\Rightarrow (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$.

1 4 6 4 1 $\Rightarrow (x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$

...

Osserviamo ad esempio l'ultimo sviluppo: se portiamo il termine x^4 a sinistra otteniamo $(x+y)^4 - x^4 = 4x^3y + 6x^2y^2 + 4xy^3 + y^4 = y \cdot (4x^3 + 6x^2y + 4xy^2 + y^3) := y \cdot m$; da questo segue che $y \mid (x+y)^4 - x^4$ e quindi, in generale, $y \mid (x+y)^n - x^n$.

Esempio. Dimostrare che $5^n - 1$ è divisibile per 4.

- Poiché $5 = 4 + 1$, possiamo scrivere $5^n - 1 = (4+1)^n - 1$. Per quanto osservato in precedenza, 4 divide $(4+1)^n - 1^n$, ovvero $5^n - 1$, come volevasi dimostrare.
- Oppure: poiché $5 \in [1] \bmod(4)$, per la proprietà "aggiuntiva" 5, tutte le potenze di 5 appartengono alla classe di resto $[1]$ modulo 4, da cui segue che 4 divide $5^n - 1$.

Un criterio per la divisibilità

La proprietà 5 permette di determinare i resti delle divisioni delle successive potenze di 10 per un numero dato. Per esempio, poiché $10 \equiv -1 \bmod(11)$, allora $10^2 \equiv (-1)^2 \bmod(11)$, e così via. Di conseguenza, se $z = a_n a_{n-1} \ldots a_0 = \sum_{k=0}^{n} a_k 10^k$, la sua classe di resto modulo 11 è

$[z] = \left[\sum_{k=0}^{11} a_k 10^k\right] = \sum_{k=0}^{n} [a_k 10^k] = \sum_{k=0}^{n} [a_k][10^k] = \sum_{k=0}^{n} a_k (-1)^k$. Morale, un numero intero è divisibile per 11 *se la somma delle cifre a segno alterno è zero.* Per esempio, $z = 121 \Rightarrow [z] = 1 - 2 + 1 = 0$.

Analogamente possiamo stabilire criteri di divisibilità per 3 o per 9. Infatti, $10 \equiv 1 \bmod(3)$, e pure $10 \equiv 1 \bmod(9)$. Questo significa che la verifica della divisibilità viene condotta sulla somma delle cifre: se questa è multipla di 3, o di 9, allora il numero è divisibile per 3 o per 9.

Come ultimo caso, studiamo la divisibilità per 7. Risulta:

$10 \equiv 3 \bmod(7) \Rightarrow 10^2 \equiv 2 \bmod(7) \Rightarrow 10^3 \equiv (-1) \bmod(7) \Rightarrow$

$10^4 \equiv (-3) \bmod(7) \Rightarrow 10^5 \equiv (-2) \bmod(7) \Rightarrow 10^6 \equiv 1 \bmod(7)$

Esercizio. Determinare a quale numero compreso tra 0 e 6 è congruo modulo 7 il numero $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$.

Esercizio. La struttura algebrica $(Z_4, \bullet)$ è un gruppo? E $(Z_5 - \{0\}, \bullet)$?

Esercizio. Dimostrare che, se p è primo, $ab \equiv 0 \bmod(p) \Leftrightarrow a \equiv 0 \bmod(p) \wedge b \equiv 0 \bmod(p)$.

- $(\Rightarrow)\ p \mid ab \Rightarrow p \mid a \wedge p \mid b \Rightarrow a \equiv 0 \bmod(p) \wedge b \equiv 0 \bmod(p)$;

- $(\Leftarrow) a \equiv 0 \bmod(p) \wedge b \equiv 0 \bmod(p) \Rightarrow ab = hp \Rightarrow ab \equiv 0 \bmod(p)$.

Il "piccolo" teorema di Fermat

Un importante criterio di divisibilità ci viene fornito dal seguente risultato.

Teorema (Fermat). Se p è primo e $p \nmid a$, allora $a^{p-1} \equiv 1 \bmod(p)$.

Dimostrazione. Costruiamo i seguenti multipli di a: $m_1 = 1 \cdot a, m_2 = 2 \cdot a, ..., m_{p-1} = (p-1) \cdot a$, e consideriamo $m_s - m_r = (s-r)a$. Poiché $p \nmid a$ e p è primo (quindi non divide $s-r$, essendo $s, r \le p-1$), nessuna coppia m_r, m_s è congrua modulo p. Inoltre, nessun m_i è congruo a zero modulo p (perché?).

Di conseguenza, preso un numero m_i, per il teorema della fattorizzazione unica, non essendo primo, deve essere divisibile per un certo intero compreso tra 1 e $p-1$ (estremi inclusi). Di conseguenza, i numeri $m_1 = 1 \cdot a, m_2 = 2 \cdot a, ..., m_{p-1} = (p-1) \cdot a$ sono congrui ai numeri $1, 2, ..., p-1$, presi in un certo ordine. Ora, poiché $m_1 \cdot m_2 \cdot ... \cdot m_{p-1} = (1 \cdot 2 \cdot ... \cdot p-1)a^{p-1}$, risulta quindi $(1 \cdot 2 \cdot ... \cdot p-1)a^{p-1} \equiv (1 \cdot 2 \cdot ... \cdot p-1) \bmod(p)$. Quindi p è un numero primo che divide il prodotto $(1 \cdot 2 \cdot ... \cdot p-1)(a^{p-1}-1)$. Ne segue che p deve quindi dividere un fattore tra $(1 \cdot 2 \cdot ... \cdot p-1)$ e $(a^{p-1}-1)$; poiché non divide il prodotto $(1 \cdot 2 \cdot ... \cdot p-1)$, deve necessariamente dividere $(a^{p-1}-1)$ e quindi $a^{p-1} \equiv 1 \bmod(p)$.

Esercizi

1. Sia $m \in N$. Definiamo l'insieme $E_m = \left\{ n \in N \mid \ 1 \le n < m, \quad MCD(n,m) = 1 \ \right\}$ formato dai numeri naturali minori di *m* primi con *m*. Dimostrare che l'insieme $Z_{12}^* = \left\{ [n] \in Z_{12} \mid n \in E_m \right\}$ è un gruppo rispetto all'operazione di moltiplicazione tra classi di resto in Z_{12}.
2. Risolvere la seguente equazione: $[18x] = [16] \bmod 40$.
3. Si stabilisca se $3^{155} + 2$ è divisibile per 7.
4. Si spieghi perché l'insieme Z_n munito dell'operazione di moltiplicazione tra classi di resto, non può essere un gruppo se *n* è un numero naturale composto. Quale struttura algebrica origina? Cosa possiamo dire, in tal senso, di $Z_n - [0]$?
5. Il numero di elementi dell'insieme $E_m = \left\{ n \in N \mid \ 1 \le n < m, \quad MCD(n,m) = 1 \ \right\}$, al variare di $m \in N$ dà origine alla funzione nota come "$\varphi(m)$ di Eulero". Si dimostri che dal *Teorema di Eulero*: "se $a < m$ e $MCD(a,m) = 1$, allora $a^{\varphi(m)} \equiv 1 \bmod m$" è possibile dedurre come corollario il celebre *Teorema di Fermat:* "se $a < p$, p primo e $MCD(a,p) = 1$, allora $a^{p-1} \equiv 1 \bmod p$.
6. Un numero è divisibile per tre se la somma delle cifre è un multiplo di tre. Giustificare quest'affermazione.
7. (Problema 25 libro di testo). Un marziano, dopo aver visto scritta l'equazione $x^2 - 16x + 41 = 0$, invitato a scrivere la differenza delle radici, scrive 10. Sapendo che i numeri tra 0 e 6 coincidono con quelli in base 10, si dica quante dita ha il marziano.
8. Si attribuisca un significato alla frazione $\frac{1}{4} \bmod(7)$.
9. Si attribuisca un significato alla frazione $\frac{1}{4} \bmod(6)$.
10. Dimostrare che per ogni $n > 0$ il numero $5^n + 2 \cdot 3^{(n-1)} + 1$ è divisibile per 8.

11. Dire a quale classe di resto modulo 5 appartiene il numero $1+2+2^2+...+2^{19}$.

12. (Problema 34 libro di testo) E' dato un cesto di uova; si sa che se si tolgono a due a due resta un uovo, se si tolgono a tre a tre ne restano due, mentre se si tolgono a quattro a quattro ne restano tre. Dire qual è il numero minimo di uova nel cesto.
13. Dimostrare che in Z_p con p primo vale l'uguaglianza $(x+y)^p = x^p + y^p$.
14. (Problema 74 libro di testo). Due cercatori d'oro hanno due grandi sacchi di pezzi d'oro. Il primo ha solo pezzi da 15 grammi, il secondo solo pezzi da 21 grammi. Può il primo pagare al secondo un debito di 27 grammi d'oro? Potrebbe il secondo pagare al primo un debito di 29 grammi d'oro?

Soluzioni

1. Dalla definizione risulta $E_{12} = \{1,5,7,11\}$. Se associamo agli elementi di E_{12} le rispettive classi di resto in Z_{12}, otteniamo l'insieme che, munito dell'operazione di prodotto in Z_n, vogliamo verificare essere un gruppo: $Z_{12}^* = \{[1],[5],[7],[11]\}$. Per questo scopo è sufficiente costruire la tavola della moltiplicazione:

Z_{12}^*	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

   - Osserviamo che l'insieme è chiuso rispetto all'operazione di moltiplicazione, che questa è associativa, che esiste l'elemento neutro ($[1]$), e che ogni elemento è inverso di se stesso.
2. $40 \mid (18x-16) \Rightarrow 18x-16 = 40y \Rightarrow 9x-20y = 8$. Le soluzioni dell'equazione omogenea sono $\begin{cases} x_0 = 20n \\ y_0 = 9n \end{cases}$, una soluzione particolare è data da $\begin{cases} x' = 9\cdot 8 = 72 \\ y' = 4\cdot 8 = 32 \end{cases}$ per cui $x = 20n+72 = 20n+32$.

3. Risulta $MCD(3,7) = 1$, 7 è un numero primo, quindi si può applicare il teorema di Fermat: $3^6 \equiv 1 \bmod 7$. Ora, $155 = 25\cdot 6 + 5 \Rightarrow [3^{155}] = [3^{25\cdot 6}\cdot 3^5] = [3^5] = [5]$. Allora $[3^{155}+2] = [5]+[2] = [0].$ Il numero $3^{155}+2$ è quindi divisibile per 7.

4. Nell'insieme Z_n munito dell'operazione di moltiplicazione tra classi di resto, ad esempio in Z_6 esiste un elemento, $[2]$, che non ha inverso rispetto alla suddetta operazione. Ciò è sufficiente per affermare che Z_6 è un *monoide associativo*, ma non un gruppo. In generale questo accade in Z_n se *n* è composto e si considera la classe di resto di un divisore primo di *n*. Per quanto riguarda $Z_n - [0]$, in base a quanto appena affermato possiamo concludere che *non* risulta chiuso rispetto alla moltiplicazione, quindi non è neppure una struttura algebrica.

5. La chiave per la soluzione del problema è rappresentata dal fatto che, se *m* è un numero primo *p*, allora *tutti* gli interi minori di *p* sono primi con *p*. Poiché tali interi sono, ovviamente, in numero di $\varphi(p) = p - 1$, allora $a^{\varphi(m)} \equiv 1 \bmod m$ è proprio la tesi del teorema.
6. Si osserva che $10 \equiv 1 \bmod 3 \Rightarrow [10] = [1] \Rightarrow [10^n] = [10]^n = [1]^n = [1]$, di conseguenza un qualsiasi numero intero $z = a_n a_{n-1} \ldots a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_0$, è tale che $[z] = [a_n + a_{n-1} + \ldots a_0]$, come volevasi dimostrare.

7. Indicato con *n* il numero di dita del marziano (si suppone che abbia due mani, ognuna con lo stesso numero di dita), ragionando come faremmo in base dieci scriviamo: $16 = 1 \cdot n^1 + 6 \cdot n^0; \quad 41 = 4 \cdot n^1 + 1 \cdot n^0; \quad 10 = 1 \cdot n + 0 \cdot n^0$. In questo modo i coefficienti dell'equazione di secondo grado sono $a = 1 = 1 \cdot n^0; \quad b = -16 = -(n+6); \quad c = 41 = (4n+1)$, e la differenza delle radici, espressa dalla condizione $x_2 - x_1 = \frac{\sqrt{\Delta}}{a} \Rightarrow 10 = n = \frac{\sqrt{(n+6)^2 - 4(4n+1)}}{1} \Rightarrow n = 8$.
8. Si tratta di trovare il "reciproco di 4 modulo 7", ovvero la classe di resto che, moltiplicata per la classe di 4, dà come risultato la classe di 1: si tratta della classe di resto modulo 2: $\frac{1}{4} \bmod(7) = [2]_7$. Infatti $[2]_7 \cdot [4]_7 = [8]_7 = [1]_7$.

9. Stavolta non è possibile attribuire un significato alla frazione. Infatti, se moltiplichiamo 4 per ognuno dei numeri da 1 a 5, non otteniamo mai un numero che, diviso per 6, dà come resto uno.
10. Dall'osservazione delle successive potenze di 5 possiamo concludere che $5^n \in [5]_8$ se *n* è dispari, oppure che $5^n \in [1]_8$ se *n* è pari. Ora, sempre per *n* pari, $3^{(n-1)} \in [3]_8$ e per *n* dispari $3^{(n-1)} \in [1]_8$. Ricapitolando, $5^n + 2 \cdot 3^{(n-1)} + 1 \in [1] + 2[3] + [1] = [0]$ se *n* è pari, e $5^n + 2 \cdot 3^{(n-1)} + 1 \in [5] + 2[1] + [1] = [0]$ se *n* è dispari. In ogni caso giungiamo al risultato cercato.
11. Osserviamo che le classi di resto a cui appartengono le potenze di 2 che costituiscono i singoli addendi si ripetono con questa periodicità: $1 \in [1] \quad 2 \in [2] \quad 4 \in [4] \quad 8 \in [3] \quad 16 \in [1] \quad 32 \in [2] \quad 64 \in [4] \quad 128 \in [3]$. La periodicità è giustificata dalle proprietà aggiuntive. Quindi la somma fino all'addendo 2^{19} avviene contando $[1] + [2] + [4] + [3] = [1 + 2 + 4 + 3] = [10] = [0]$ esattamente 5 volte. La somma è quindi divisibile per 5, quindi appartiene alla classe di resto 0.

12. Il numero minimo di uova N appartiene alla classe di resto 1 modulo due, a quella 2 modulo tre, e a quella 3 modulo quattro: $N \in [1]_2 \Rightarrow N = 2m + 1; \quad N \in [2]_3 \Rightarrow N = 3n + 2; \quad N \in [3]_4 \Rightarrow N = 4k + 3$. I numeri di uova possibili si ottengono risolvendo le equazioni diofantee (a soluzioni intere!) che si ottengono uguagliando le espressioni sopra: $\begin{cases} 2m - 3n = 1 \\ 2m - 4k = 2 \Rightarrow m - 2k = 1 \end{cases}$. Dalla prima equazione segue, ad esempio, $m = 5$ e $n = 3$. Sostituendo nella seconda equazione otteniamo $k = 2$. Per questi valori risulta $N = 11$.

13. Per il teorema di Fermat risulta $x^p \equiv x \bmod(p)$ e $y^p \equiv y \bmod(p)$. Di conseguenza $\left(x^p + y^p\right) \equiv (x+y) \bmod(p)$ e, poiché, sempre per il teorema di Fermat, $(x+y)^p \equiv (x+y) \bmod(p)$, la tesi segue per la proprietà transitiva.

14. Nella transazione (con resto) indicati con *x* e con *y* il numero di pezzi rispettivamente da 15 e da 21 grammi, per rispondere alla domanda occorre risolvere l'equazione diofantea $15x - 21y = 27 \Rightarrow 5x - 7y = 9$. Le soluzioni sono $x = 3$ e $y = 2$. Nel secondo caso, poiché $MCD(15,21) = 3$ non divide 29, l'equazione risolvente $21y - 15x = 29$ non ha soluzioni intere; il pagamento non può quindi avvenire.

Approfondimento: la divisibilità per tre, e il numero minimo di pesate con la bilancia a bracci uguali

Vogliamo risolvere il seguente problema: qual è il numero *minimo* di masse campione necessario per misurare con una bilancia a bracci uguali una massa non superiore ai 1000g?
Una risposta a questa domanda può essere data interpretando opportunamente i *resti* nella divisione per tre. Infatti, ogni numero nella divisione per tre può dare come resto 0, 1, 2. Ora, se osserviamo che $-1 = 2 - 3$, possiamo suddividere tutti i numeri interi nelle cosiddette *classi di resto* $[-1],[0],[1]$, ed esprimere così ogni numero tra 1 e 1000 in base 3.
Quindi, ogni valore numerico di massa è ottenibile combinando opportunamente masse campione da $3^n g$, con $3^n \le 1000$, ovvero $n = 6$, dal momento che $3^7 = 2187 > 1000$. La nostra pesiera "ideale" è dunque costituita da masse campione di $\{1,3,9,27,81,243,729\}g$.

Qual è l'idea che sta alla base del ragionamento? La risposta ci viene suggerita dalla bilancia stessa, in quanto una volta posta la massa da misurare su uno dei due bracci, per esempio quello di sinistra, possiamo raggiungere l'equilibrio mettendo le masse campione sui due bracci. In questo modo "-1" rappresenta le masse che vengono poste sul braccio dove si trova la massa da misurare, e "1" quelle che vengono poste sull'altro braccio. Vediamo come funziona il tutto con un esempio.
Se vogliamo misurare una massa da 378g dobbiamo procedere così:
$243 < 378 < 729$ e $378 > 1+3+9+27+81+243 = 364$ quindi metteremo la massa da 729g sull'altro piatto: $729 - 378 = 351$. Il peso da 729g non possiamo più utilizzarlo. Si ha, anzi si deve necessariamente avere, $351 < 1+3+9+27+81+243 = 364$, quindi $351 - 243 = 108$, il peso da 243g viene messo sullo stesso piatto della massa da misurare. A questo punto $108 = 81 + 27$: siamo stati fortunati, poniamo le masse da 81g e da 27g sullo stesso piatto della massa da misurare ed il gioco è fatto. Riassumendo:

$$\begin{cases} 378 = 729 - 351 \\ 351 = 243 + 108 \\ 108 = 81 + 27 \end{cases} \Rightarrow 378 = 729 - 243 - 81 - 27 \Rightarrow 378 + 243 + 81 + 27 = 729 .$$