

Capitolo 4

Aritmetica Modulare

4.1 Gli interi modulo n

Sia n un intero e consideriamo la relazione \mathfrak{R}_n in Z cosí definita:

$$a\mathfrak{R}_nb \Leftrightarrow a - b = hn, \text{ per qualche intero } h \in Z.$$

La relazione \mathfrak{R}_n risulta d'equivalenza (cfr.eserc.3.3.4) e si chiama *congruenza modulo n* . Per indicare che a é nella relazione \mathfrak{R}_n con b si scrive anche $a \equiv b(\text{mod } n)$ e si legge *a é congruo*, o *congruente*, a b modulo n .

DEFINIZIONE 4.1.1 L'insieme quoziente Z/\mathfrak{R}_n si denota con Z_n , o con Z/nZ , e si chiama *insieme degli interi modulo n* . La classe d'equivalenza di un elemento $a \in Z$ rispetto ad \mathfrak{R}_n si denota con $[a]_{\mathfrak{R}_n}$ o piú semplicemente con $[a]$, se non vi é luogo ad equivoci. \diamond

Poiché risulta

- $n = 0 \Rightarrow \mathfrak{R}_0$ é la relazione di uguaglianza in Z .
- $n = 1 \Rightarrow a\mathfrak{R}_1b$, per ogni $a, b \in Z \Rightarrow [a]_{\mathfrak{R}_1} = [b]_{\mathfrak{R}_1} = Z$, per ogni $a, b \in Z$;
- $\mathfrak{R}_n = \mathfrak{R}_{-n}$;

nel seguito supporremo sempre $n > 1$.

Per la congruenza modulo n valgono le seguenti proprietá e osservazioni:

- $[0] = \{hn : h \in Z\}$ (questo insieme si denota anche con nZ).
- $a \neq 0 \Rightarrow [a] = \{a + hn : h \in Z\}$ (questo insieme si denota anche con $a + nZ$).
- $0 \leq a < n \Rightarrow n - a \equiv -a(\text{mod } n)$.
- $r =$ resto della divisione tra a ed $n \Rightarrow a \equiv r(\text{mod } n)$.
- Il numero delle *classi di congruenza* modulo n é esattamente n e risulta

$$Z_n = \{[0], [1], \dots, [n - 1]\}.$$

OSSERVAZIONE 4.1.2 In forza dell'ultima proprietà abbiamo che, per ogni intero a , il più piccolo intero non negativo appartenente ad $[a]_{\mathbb{R}_n}$ è il resto della divisione di a per n . In altre parole, le classi d'equivalenza modulo n sono in corrispondenza biunivoca con i possibili resti della divisione per n e, quindi, possono identificarsi con questi. Per tale motivo esse si chiamano anche *classi dei resti modulo n* e nel seguito, se non vi è luogo ad equivoci, saranno denotate semplicemente con $0, 1, \dots, n-1$, omettendo le parentesi quadre. Più in generale, con abuso di notazione, spesso scriveremo a in luogo di $[a]$, per ogni intero a .

In molti testi il resto r della divisione di a per n è denotato col simbolo $a \bmod n$. In questo caso le scritture $b = a \bmod n$ e $b \equiv a \bmod n$ hanno significato diverso: la prima dice che $b = r$, la seconda che $b - a$ è un multiplo di n . \diamond

Altre due importanti proprietà, che si consiglia di dimostrare per esercizio, sono:

- $x, x' \in [a], y, y' \in [b] \Rightarrow [x + y] = [x' + y']$.
- $x, x' \in [a], y, y' \in [b] \Rightarrow [xy] = [x'y']$.

Queste assicurano che in Z_n le seguenti operazioni di *addizione* e *moltiplicazione* risultano *ben definite*¹:

$$[a] + [b] = [a + b] \quad , \quad [a][b] = [ab].$$

Le operazioni di addizione e moltiplicazione in Z_n verificano le seguenti *proprietà fondamentali*:

- $([a] + [b]) + [c] = [a] + ([b] + [c])$,
- $[a] + [0] = [0] + [a] = [a]$,
- $[a] + [-a] = [0]$,
- $[a] + [b] = [b] + [a]$,
- $([a][b])[c] = [a]([b][c])$,
- $[a][1] = [1][a] = [a]$,
- $[a][b] = [b][a]$,
- $([a] + [b])[c] = [a][c] + [b][c]$,

OSSERVAZIONE 4.1.3 Il fatto che valgono le sopraelencate proprietà si esprime dicendo che Z_n , rispetto alle operazioni di addizione e moltiplicazione, è un *anello commutativo unitario* nel quale lo *zero* è $[0]$ e l'*unità* è $[1]$. Lo studio di questo anello si chiama *aritmetica modulo n* , o *aritmetica modulare*. \diamond

Riportiamo come esempi le tabelline delle operazioni (*tablette di Cayley*) di Z_2, Z_3, Z_4, Z_5 .

TABELLE DI CAYLEY DI Z_2

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

¹Questo significa che le due operazioni non dipendono dai rappresentanti delle classi scelte ma soltanto da queste ultime.

TABELLE DI CAYLEY DI Z_3

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

TABELLE DI CAYLEY DI 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

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

TABELLE DI CAYLEY DI Z_5

+	0	1	2	3	4
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

·	0	1	2	3	4
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

OSSERVAZIONE 4.1.4 L'aritmetica modulo 2 si presta a svariate applicazioni perché é riproducibile mediante i due possibili stati di alcuni sistemi fisici per i quali il passaggio da uno stato all'altro é regolato dall'addizione o dalla moltiplicazione in Z_2 . Ad esempio, se ad un circuito elettrico facciamo corrispondere 0 quando é aperto e 1 quando é chiuso, le operazioni definite su Z_2 possono realizzarsi usando i circuiti descritti nella figura 4.1. ◇

Figura 4.1:

ESERCIZIO 4.1.5 Sia

$$n = r_m 10^m + r_{m-1} 10^{m-1} + \cdots + r_2 10^2 + r_1 10 + r_0.$$

Provare che risulta $n \equiv r_m + r_{m-1} + \cdots + r_2 + r_1 + r_0 \pmod{9}$.

SOLUZIONE. Si ha:

$$\bullet 10^m - 1 = \underbrace{999 \cdots 9}_m = 9 \cdot 10^{m-1} + 9 \cdot 10^{m-2} + \cdots + 9 \cdot 10^2 + 9 \cdot 10 + 9$$

$$\Rightarrow 10^m - 1 \equiv 0 \pmod{9}.$$

$$\bullet n - (r_m + r_{m-1} + \cdots + r_2 + r_1 + r_0) =$$

$$(r_m 10^m + \cdots + r_1 10 + r_0) - (r_m + \cdots + r_1 + r_0) =$$

$$(10^m - 1)r_m + \cdots + (10^2 - 1)r_2 + (10 - 1)r_1 \equiv 0 \pmod{9}. \quad \diamond$$

ESERCIZIO 4.1.6 Dimostrare i seguenti criteri di divisibilit :

- un intero   divisibile per 2 se, e solo se, la sua ultima cifra decimale   pari;
- un intero   divisibile per 3 se, e solo se, la somma delle sue cifre decimali   divisibile per 3;
- un intero   divisibile per 4 se, e solo se, l'intero corrispondente alle sue ultime due cifre decimali   divisibile per 4;
- un intero   divisibile per 5 se, e solo se, la sua ultima cifra decimale   divisibile per 5;
- un intero   divisibile per 9 se, e solo se, la somma delle sue cifre decimali   divisibile per 9;
- un intero   divisibile per 2^h se, e solo se, l'intero corrispondente alle sue ultime h cifre decimali   divisibile per 2^h .

ESERCIZIO 4.1.7 Provare che un intero   divisibile per 11 se, e solo se, la somma a segni alterni delle cifre nella sua rappresentazione decimale   divisibile per 11 (si tenga presente che $10 \equiv -1 \pmod{11}$).

ESERCIZIO 4.1.8 Trovare il resto della divisione per 9 di un intero del tipo 83^{6a} .

SOLUZIONE. Si tratta di trovare l'unico intero r compreso fra 0 e 9 tale che

$$83^{6a} \equiv r \pmod{9}.$$

Poich   

$$83 \equiv 2 \pmod{9},$$

risulta

$$83^{6a} \equiv 2^{6a} \pmod{9}.$$

D'altra parte, essendo

$$2^{6a} = (2^6)^a \quad \text{e} \quad 2^6 \equiv 1 \pmod{9},$$

²Si noti che questo esercizio   alla base della *prova del nove*, regola che si impara alle scuole elementari per controllare la correttezza del risultato della moltiplicazione fra due interi.

abbiamo

$$2^{6a} \equiv 1 \pmod{9}.$$

Ne segue che

$$83^{6a} \equiv 1^a \equiv 1 \pmod{9},$$

così il resto cercato é 1. ◇

4.2 Funzione di Eulero e piccolo teorema di Fermat

Diverse proprietà di un intero $n > 1$ dipendono, oltre che dalla sua fattorizzazione in primi, anche dal numero di interi compresi fra 1 ed n e coprimi con n . É questa la motivazione per la seguente definizione.

DEFINIZIONE 4.2.1 Per un intero $n > 1$ si denota con $\Phi(n)$ il numero degli interi positivi minori di n e coprimi con esso. La funzione Φ si chiama *funzione di Eulero*. ◇

ESERCIZIO 4.2.2 *Provare che $\Phi(n) = n - 1$ se, e solo se, n é primo.*

PROPOSIZIONE 4.2.3 *Per ogni primo positivo p e per ogni intero $h > 0$, risulta*

$$\Phi(p^h) = p^h - p^{h-1}. \quad (4.1)$$

DIMOSTRAZIONE. Gli interi positivi minori di p^h che non sono coprimi con p^h sono tutti e soli quelli del tipo mp , con $1 \leq m \leq p^{h-1}$, e da ciò segue l'asserto. ◇

PROPOSIZIONE 4.2.4 *Se p e q sono primi positivi distinti, risulta*

$$\Phi(p^h q^k) = \Phi(p^h) \Phi(q^k) = p^h q^k \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right),$$

per ogni $h, k \in \mathbb{N}$.

DIMOSTRAZIONE. É lasciata per esercizio al Lettore. ◇

COROLLARIO 4.2.5 *Se a, b sono due interi positivi coprimi, risulta*

$$\Phi(a, b) = \Phi(a) \Phi(b).$$

PROPOSIZIONE 4.2.6 *Sia $n > 1$ un intero e siano p_1, p_2, \dots, p_h i primi positivi che dividono n . Allora risulta*

$$\Phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_h}\right). \quad (4.2)$$

DIMOSTRAZIONE. É un immediato corollario delle due precedenti proposizioni. ◇

Denotiamo, ora, con Z_n^* l'insieme degli elementi non nulli di Z_n .

DEFINIZIONE 4.2.7 Un elemento $a \in Z_n^*$ si dice *invertibile* se esiste un elemento $b \in Z_n^*$ tale che $ab = 1$. In questo caso b si chiama *inverso* di a e si denota con a^{-1} . L'insieme degli elementi invertibili di Z_n si denota con $U(n)$. ◇

TEOREMA 4.2.8 *Un elemento $a \in Z_n^*$ è invertibile se, e solo se, a ed n sono coprimi in Z .*

DIMOSTRAZIONE. Si ha:

- $ax = 1$ in $Z_n \Rightarrow ax \equiv 1(\text{mod } n) \Rightarrow ax - 1 = hn$, per qualche $h \in Z \Rightarrow ax - hn = 1 \Rightarrow MCD(a, n) = 1$.
- $MCD(a, n) = 1 \Rightarrow ha + kn = 1$, per qualche $h, k \in Z \Rightarrow ha - 1 = -kn \Rightarrow ha \equiv 1(\text{mod } n) \Rightarrow ha = 1$ in Z_n . ◇

COROLLARIO 4.2.9 *Il numero degli elementi invertibili di Z_n^* è uguale a $\Phi(n)$.*

COROLLARIO 4.2.10 *Gli elementi di Z_n^* sono tutti invertibili se, e solo se, n è un primo. In tal caso Z_n è un campo.*

OSSERVAZIONE 4.2.11 *Se a ed n sono coprimi, il calcolo di a^{-1} in Z_n può effettuarsi andando a trovare una soluzione (b, h) in Z dell'equazione (cfr.2.3.16)*

$$ax + ny = 1.$$

Per (b, h) , infatti, risulta $ab = 1 - nh$; cioè $b = a^{-1}$ in Z_n . Facciamo presente che esistono algoritmi efficienti per risolvere la precedente equazione. ◇

OSSERVAZIONE 4.2.12 *In Z_n può accadere che il prodotto di due elementi diversi da zero sia uguale a zero, cioè che non valga la legge di annullamento del prodotto. Per esempio, in Z_6 risulta $[2][3] = [0]$ ed è $[2] \neq [0]$ e $[3] \neq [0]$.* ◇

ESERCIZIO 4.2.13 *Provare che in Z_n vale la legge di annullamento del prodotto se, e solo se, l'intero n è primo.*

DEFINIZIONE 4.2.14 *Un elemento $a \in Z_n$ si dice divisore dello zero se esiste un elemento $b \neq 0$ tale che $ab = 0$.* ◇

PROPOSIZIONE 4.2.15 *Un elemento $a \in Z_n$ è divisore dello zero se, e solo se, a ed n non sono coprimi.*

DIMOSTRAZIONE. Se a ed n non sono coprimi, per $d = MCD(a, n)$, abbiamo $1 < d \leq n$, così $b = n/d$ è minore di n e risulta $ab = 0$ in Z_n . Se $ab = 0$, con $0 < a, b < n$, allora n non divide a , non divide b e divide ab ; ne segue che $MCD(a, n) \neq 1$. ◇

ESERCIZIO 4.2.16 *Provare che il prodotto di due elementi di $U(n)$ è un elemento di $U(n)$.*

TEOREMA 4.2.17 (teorema di Fermat-Eulero) *Siano a, n due interi positivi coprimi con $n > 1$. Allora risulta*

$$a^{\Phi(n)} \equiv 1(\text{mod } n). \tag{4.3}$$

DIMOSTRAZIONE. Cominciamo con l'osservare che, se $y \in U(n)$ e poniamo

$$yU(n) = \{yx \quad : \quad x \in U(n)\},$$

risulta $yU(n) = U(n)$. Posto, allora, $k = \Phi(n)$, sia

$$U(n) = \{x_1, x_2, \dots, x_k\}$$

e poniamo $y = x_1 x_2 \cdots x_k$. Poiché $a \in U(n)$ e $aU(n) = U(n)$, in Z_n abbiamo

$$y = x_1 x_2 \cdots x_k = (ax_1)(ax_2) \cdots (ax_k) = a^k y.$$

Essendo y invertibile in $U(n)$, possiamo moltiplicare l'ultima uguaglianza per y^{-1} e otteniamo che

$$1 = a^k$$

in Z_n , come volevamo dimostrare. \diamond

OSSERVAZIONE 4.2.18 Il teorema di Fermat-Eulero, asserendo che

$$aa^{\Phi(n)-1} = a^{\Phi(n)} \equiv 1(\text{mod } n)$$

quando l'intero a é coprimo con n , può anche riformularsi dicendo che in Z_n , se un elemento b é invertibile, risulta $b^{-1} = b^{\Phi(n)-1}$. Questa osservazione chiarisce che il calcolo dell'inverso di b in Z_n attraverso la (4.3) richiede la conoscenza di $\Phi(n)$ e, quindi, della fattorizzazione in primi di n . \diamond

TEOREMA 4.2.19 (piccolo teorema di Fermat) *Sia p un primo positivo. Allora risulta*

$$a^p \equiv a(\text{mod } p), \quad \text{per ogni intero positivo } a; \quad (4.4)$$

o, equivalentemente,

$$a^{p-1} \equiv 1(\text{mod } p), \quad \text{per ogni intero positivo } a \text{ non divisibile per } p. \quad (4.5)$$

DIMOSTRAZIONE. Se p non divide a , abbiamo $\Phi(p) = p - 1$ e quindi $a^{p-1} = a^{\Phi(p)}$. Ne segue, per il teorema di Fermat-Eulero, che $a^{p-1} \equiv 1(\text{mod } p)$ e quindi $a^p \equiv a(\text{mod } p)$. Se p divide a , la (4.4) é banale. \diamond

COROLLARIO 4.2.20 *Se p é un primo positivo e b un elemento non nullo di Z_p , risulta*

$$b^{-1} = b^{p-2}; \quad (4.6)$$

o, equivalentemente,

$$a^{p-1} \equiv 1(\text{mod } p), \quad \text{per ogni intero positivo } a < p. \quad (4.7)$$

OSSERVAZIONE 4.2.21 Il piccolo teorema di Fermat, per ogni intero positivo $a < m$, dá una condizione necessaria (che nell'antica Cina, per $a = 2$, si riteneva fosse anche sufficiente) affinché un intero positivo $m > 1$ sia primo:

$$m \text{ primo} \Rightarrow m \mid (a^m - a).$$

Purtroppo queste condizioni non sono sufficienti e i primi due controesempi, per $a = 2$, sono $m = 341 = 11 \cdot 31$ (diciottesimo secolo) e $m = 561 = 3 \cdot 11 \cdot 17$. Gli interi $m > 1$ che verificano il "test cinese" per un fissato a , cioè tali che $m \mid (a^m - a)$, prendono il nome di *pseudoprimi* in base a . Più in generale si ha che il piccolo teorema di Fermat non é invertibile e, quindi, non può essere utilizzato come test di primalità. Esistono, infatti, interi non primi $m > 1$, divisibili per $a^m - a$, per ogni intero positivo $a < m$. Questi sono noti come *numeri di Carmichael* e i primi due esempi sono 561 e $1729 = 7 \cdot 13 \cdot 19$. \diamond

4.3 Congruenze lineari

Se a, b, m sono interi con $m > 1$, l'equazione in x

$$ax \equiv b \pmod{m} \tag{4.8}$$

prende il nome di *equazione congruenziale lineare*, o *congruenza lineare*, e una sua soluzione é, per definizione, un intero \bar{x} tale che $a\bar{x} \equiv b \pmod{m}$. Osserviamo che l'essere \bar{x} una soluzione della (4.8) equivale all'esistenza di un intero n tale che $a\bar{x} - b = nm$, cioè $a\bar{x} - mn = b$. Allora la prop.2.3.16 equivale alla seguente proposizione.

PROPOSIZIONE 4.3.1 La congruenza lineare (4.8) ha soluzioni se, e solo se, $MCD(a, m)$ divide b .

PROPOSIZIONE 4.3.2 Nell'ipotesi che l'equazione (4.8) abbia una soluzione c , poniamo $d = MCD(a, m)$ e $m = dm_1$. Allora le soluzioni della (4.8) sono tutte e sole quelle del tipo

$$\bar{x} = c + nm_1, \quad n \in \mathbb{Z}. \tag{4.9}$$

DIMOSTRAZIONE. É simile a quella della prop.2.3.17 ed é lasciata per esercizio al Lettore. \diamond

PROPOSIZIONE 4.3.3 Nell'ipotesi che l'equazione (4.8) sia risolubile, poniamo $d = MCD(a, m)$, $m = dm_1$ e sia c una sua soluzione. Allora, le soluzioni della (4.8) a due a due incongrue modulo m sono esattamente d e precisamente:

$$c, c + m_1, c + 2m_1, \dots, c + (d - 1)m_1. \tag{4.10}$$

DIMOSTRAZIONE. E' chiaro che le soluzioni (4.10) sono a due a due incongrue modulo m . Sia, dunque, $c + nm_1$ una soluzione della (4.8) e sia $n = dq + r$, con q, r quoziente e resto della divisione di n per d . Allora é $0 \leq r < d$,

$$c + nm_1 = c + (dq + r)m_1 = c + dqm_1 + rm_1 = c + qm + rm_1 \equiv c + rm_1 \pmod{m}$$

e l'asserto é completamente provato. \diamond

TEOREMA 4.3.4 (teorema di cinese del resto) Siano m_1, m_2 interi maggiori di 1 tali che $MCD(m_1, m_2) = 1$. Allora il sistema di congruenze lineari

$$\begin{cases} x \equiv b_1(\text{mod } m_1) \\ x \equiv b_2(\text{mod } m_2) \end{cases} \quad (4.11)$$

ammette soluzioni, che risultano a due a due congruenti modulo $m_1 m_2$. Più precisamente, se c é una soluzione del sistema, le sue soluzioni sono tutti e soli gli interi del tipo $c + nm_1 m_2$, con $n \in \mathbb{Z}$.

DIMOSTRAZIONE. Gli interi m_1 e m_2 , in forza del teorema 4.2.8, sono invertibili rispettivamente in \mathbb{Z}_{m_2} e \mathbb{Z}_{m_1} . Esistono, quindi, due interi c_1 e c_2 tali che $c_1 m_2 \equiv 1(\text{mod } m_1)$ e $c_2 m_1 \equiv 1(\text{mod } m_2)$. Allora, l'intero

$$c = b_1 c_1 m_2 + b_2 c_2 m_1$$

é una soluzione del sistema (4.11), avendosi

$$c = b_1 c_1 m_2 + b_2 c_2 m_1 \equiv b_1 c_1 m_2(\text{mod } m_1) \equiv b_1(\text{mod } m_1)$$

e

$$c = b_1 c_1 m_2 + b_2 c_2 m_1 \equiv b_2 c_2 m_1(\text{mod } m_2) \equiv b_2(\text{mod } m_2).$$

Ora, se c é una fissata soluzione del sistema (4.11), si ha subito che sono soluzioni anche gli interi del tipo $c + nm_1 m_2$, con $n \in \mathbb{Z}$. Inoltre, se \bar{c} é un'ulteriore soluzione, si ha che $\bar{c} - c$ é divisibile per $m_1 m_2$, essendo m_1 e m_2 coprimi, e quindi $\bar{c} = c + nm_1 m_2$, per un opportuno intero n . L'asserto é cosí completamente provato. \diamond

Del precedente teorema si prova facilmente la seguente generalizzazione.

TEOREMA 4.3.5 Siano m_1, m_2, \dots, m_t interi maggiori di 1 e a due a due coprimi. Allora il sistema di congruenze lineari

$$\begin{cases} x \equiv b_1(\text{mod } m_1) \\ x \equiv b_2(\text{mod } m_2) \\ \dots \\ x \equiv b_t(\text{mod } m_t) \end{cases} \quad (4.12)$$

ammette soluzioni, che risultano a due a due congruenti modulo $m_1 m_2 \cdots m_t$. Più precisamente, se c é una soluzione del sistema, le sue soluzioni sono tutti e soli gli interi del tipo

$$c + nm_1 m_2 \cdots m_t, \text{ con } n \in \mathbb{Z}.$$

4.4 Esercizi

4.4.1 Provare che il quadrato di ogni intero é congruente a 0 o ad 1 modulo 4.

4.4.2 Provare che, per ogni intero n , risulta $n^3 \equiv n(\text{mod } 6)$.

4.4.3 Provare che, per ogni intero dispari n , risulta $n^2 \equiv 1(\text{mod } 8)$.

4.4.4 Provare che la relazione su Z definita da

$$m \mathfrak{R} n \Leftrightarrow m^2 \equiv n^2 \pmod{6}$$

é d'equivalenza.

4.4.5 Provare che valgono le seguenti relazioni, senza eseguire direttamente le moltiplicazioni in esse indicate.

$$21457337 \cdot 191213 \equiv 1 \pmod{10}, \quad 32578 \cdot 23989 \equiv 17 \pmod{25}.$$

4.4.6 Stabilire se le seguenti equazioni ammettono soluzioni intere e, in caso positivo, determinare l'insieme delle soluzioni:

$$\begin{aligned} 18x + 105y = 5, & \quad 504x + 672y = 18, \\ 760x + 135y = 5, & \quad 1732x + 864y = 48. \end{aligned}$$

4.4.7 Risolvere, se é possibile, le seguenti congruenze lineari:

$$\begin{aligned} 9x &\equiv 6 \pmod{12}, & 6x &\equiv 5 \pmod{4}, & 12x &\equiv 15 \pmod{39}, \\ 6x &\equiv 5 \pmod{7}, & 24x &\equiv 21 \pmod{9}, & 3x &\equiv 1 \pmod{14}. \end{aligned}$$

4.4.8 Dire se i seguenti sistemi di congruenze lineari

$$\left\{ \begin{array}{l} x \equiv 7 \pmod{9} \\ x \equiv 3 \pmod{5} \end{array} \right. , \quad \left\{ \begin{array}{l} x \equiv 5 \pmod{10} \\ x \equiv 7 \pmod{11} \end{array} \right.$$

ammettono soluzioni e, in caso positivo, determinarle.

4.4.9 Provare che l'equazione $x^2 + y^2 = 3$ non ha soluzioni in Z_4 .

4.4.10 Elencare gli elementi invertibili di Z_4, Z_5, Z_6, Z_7, Z_8 .

4.4.11 Trovare gli inversi di 2 in Z_{11} , 7 in Z_{15} e Z_{16} , 5 in Z_{13} .

4.4.12 Provare che, per ogni intero $n > 2$, esistono almeno due elementi invertibili in Z_n che verificano l'equazione $x^2 = 1$. Quanti ne esistono esattamente nel caso n sia primo?

4.4.13 Provare che in Z_8 esistono tre elementi invertibili che verificano l'equazione $x^2 = 1$.

4.4.14 Trovare un collegamento tra l'orologio e l'aritmetica modulo 12.