ELEMENTI DI TEORIA DEI NUMERI

1. Richiami di teoria

Con $\mathbb{Z}$ indichiamo l' insieme dei numeri relativi.

Cominciamo con il ricordare la definizione di quoziente e resto della divisione di due numeri in $\mathbb{Z}$.

Definizione 1. *Siano $a, b \in \mathbb{Z}$ due interi, con $b \neq 0$. Si chiamano quoziente e resto della divisione di a per b gli interi q ed r, rispettivamente, che verificano entrambe le seguenti condizioni:*

(1) $a = qb + r$;
(2) $0 \leq r < b$.

Se la prima condizione è naturalmente associata al concetto di divisione, la seconda condizione è anch' essa naturale se si vuole che quoziente e resto siano univocamente individuati, come mostra il seguente esempio.

Esempio 2. Siano $a = 16, b = 5$. Il quoziente ed il resto della divisione di a per b sono $q = 3, r = 1$. D' altra parte, è vera anche le uguaglianze $16 = 2 \cdot 5 + 6$ e $16 = 4 \cdot 5 - 4$ che verificano la prima delle due condizioni sul quoziente ed il resto, ma non la seconda.

Definizione 3. *Siano $a, b \in \mathbb{Z}$ due interi con $b \neq 0$. Diciamo che b divide a e scriviamo $b|a$ se il resto della divisione di a per b è zero.*

Possiamo ora definire i numeri primi.

Definizione 4. *Un numero $p \in \mathbb{Z}, p > 0$, è primo se è divisibile solo per $\pm 1, \pm p$.*

I numeri primi sono i blocchi elementari che permettono di costruire tutti gli altri numeri interi. Vale infatti il seguente risultato:

Teorema 5. *Ogni numero intero si scrive in modo unico come prodotto di potenze di numeri primi.*

Dimostrazione. Possiamo ragionare sui numeri interi positivi, essendo analoga la dimostrazione per i numeri negativi.

Cominciamo col provare che una simile decomposizione esiste. A tale scopo, procediamo per induzione su a.

Se $a = 1$, allora esso è primo e quindi l' asserto è vero. Supponiamo che l' asserto sia vero per tutti i numeri minori di a, e dimostriamolo per a. Se a è primo, l' asserto è vero. Se a non è primo, allora esistono $b, c \in \mathbb{N}$ con $1 < b < a, 1 < c < a$ tali che $a = b \cdot c$. Essendo b e c minori di a per essi vale l' asserto e quindi $b = p_1^{m_1} \cdots p_r^{m_r}$ e $c = q_1^{n_1} \cdots q_s^{n_s}$ con $p_1, \ldots p_r, q_1, \ldots, q_s$ numeri primi ed $m_1, \ldots, m_r, n_1, \ldots, n_s$ interi positivi. Allora $a = p_1^{m_1} \cdots p_r^{m_r} \cdot q_1^{n_1} \cdots q_s^{n_s}$, e l' asserto vale anche per a.

Verifichiamo ora l' unicità della decomposizione. Sia

$$a = p_1^{m_1} \cdots p_r^{m_r} = q_1^{n_1} \cdots q_s^{n_s}.$$

Poiché p_1 divide a allora esso divide anche $q_1^{n_1} \cdots q_s^{n_s}$ e quindi divide uno dei numeri primi $q_1, \ldots, q_s$, ossia p_1 è uguale ad uno tra i primi $q_1, \ldots, q_s$. Supponiamo $p_1 = q_1$.

Semplificando le potenze di p_1 e q_1 (che hanno lo stesso esponente altrimenti p_1 dovrebbe dividere un prodotto in cui esso non compare), otteniamo l' uguaglianza

$$p_2^{m_2} \cdots p_r^{m_r} = q_2^{n_2} \cdots q_s^{n_s}.$$

Iterando l' argomento precedente, otteniamo che le due fattorizzazioni sono uguali. □

Possiamo allora definire massimo comun divisore e minimo comune multiplo di una coppia di interi.

Definizione 6. *Siano $a, b \in \mathbb{N}$ due interi. Si chiama massimo comun divisore di a, b e lo si indica come $MCD(a, b)$ il massimo intero che divide sia a sia b. Si chiama minimo comune multiplo di a e b, e lo si indica come $mcm(a, b)$ il minimo intero che è diviso sia da a sia da b.*

Si può dimostare che minimo comune multiplo e massimo comun divisore esistono e sono unici. Infatti, date le fattorizzazioni di a e b come potenze di numeri primi, il massimo comun divisore di a e b è il prodotto dei primi comuni elevati al minimo esponente, mentre il minimo comune multiplo è il prodotto dei primi comuni e non comuni elevati al massimo esponente. Poiché però fattorizzare un intero è un procedimento piuttosto laborioso, mostriamo un metodo alternativo di calcolo per il massimo comun divisore ed il minimo comune multiplo di due interi a, b.

Proposizione 7. *Siano a, b due interi non nulli. Allora*

$$mcm(a, b)MCD(a, b) = ab.$$

Dimostrazione. Il prodotto $mcm(a, b)MCD(a, b)$ è uguale al prodotto dei primi che compaiono nelle fattorizzazioni di a, b elevati alla somma degli esponenti, e quindi è uguale al prodotto di a e b. □

Vediamo allora come calcolare il massimo comun divisore con un algoritmo dovuto ad Euclide.

Proposizione 8. *Siano a, b due interi non nulli. Siano $a = r_0, b = r_1$ e sia r_{i+1} il resto della divisione di r_{i-1} per r_i con $i \geq 1$. Allora $MCD(a, b) = r_k$, essendo k il primo indice per cui $r_{k+1} = 0$.*

Inoltre, vale il seguente risultato:

Teorema 9. *Siano a, b due interi non nulli. Allora esistono interi r ed s che verificano l' uguaglianza*

$$MCD(a, b) = ar + bs.$$

Invece di dimostrare i risultati precedenti, li illustriamo su un esempio.

Esempio 10. Siano $a = 143, b = 121$. Dividendo a per b otteniamo

$$143 = 1 \cdot 121 + 22$$

e quindi $r_2 = 22$. Dividiamo ora b per r_2 ed otteniamo

$$121 = 5 \cdot 22 + 11$$

e quindi $r_3 = 11$. Dividiamo ora r_2 per r_3 ed otteniamo

$$22 = 2 \cdot 11 + 0$$

e quindi $r_4 = 0$ e l' algoritmo si arresta. Inoltre, $MCD(143, 121) = 11$ essendo 11 l' ultimo resto non nullo.

Esprimiamo ora 11 come combinazione di 143 e 121. La prima divisione effettuata ci dice che $143 = 1 \cdot 121 + 22$, e quindi $22 = 143 - 1 \cdot 121$. Sostituendo nella seconda divisione, otteniamo $121 = 5 \cdot (143 - 1 \cdot 121) + 11$ da cui $121 = 5 \cdot 143 - 5 \cdot 121 + 11$ ossia

$$11 = -5 \cdot 143 + 6 \cdot 121.$$

Consideriamo ora equazioni a coefficienti interi, e chiediamoci quando esse hanno soluzioni intere. Tali equazioni vengono dette Diofantee. Per semplicità ci limitiamo ad equazioni lineari.

Cominciamo da un' equazione del tipo

$$ax = b. \tag{1}$$

Proposizione 11. *L' equazione $ax = b$ con $a, b \in \mathbb{Z}, a \neq 0$, ha soluzioni in $\mathbb{Z}$ se, e solo se, $a|b$. In tal caso, la soluzione è unica ed è $x = b/a$.*

Dimostrazione. Se $c \in \mathbb{Z}$ è soluzione allora $b = ac$ e quindi $a|b$. Viceversa, se $a|b$, allora $b = ac$ per qualche $c \in \mathbb{Z}$ e quindi c è soluzione dell' equazione. L' unicità è evidente come anche la forma della soluzione. □

Trattiamo ora un' equazione lineare a due incognite.

Proposizione 12. *L' equazione*

$$ax + by = c \tag{2}$$

ha soluzioni intere se, e solo se, $MCD(a, b)|c$. In questo caso, le soluzioni sono infinite e dipendono da un parametro libero in $\mathbb{Z}$.

Dimostrazione. Sia $(x_0, y_0) \in \mathbb{Z}^2$ una soluzione, ossia $ax_0 + by_0 = c$. Poiché $MCD(a, b)|a$ e $MCD(a, b)|b$ allora $MCD(a, b)|ax_0 + by_0 = c$. Viceversa, sia $c = qMCD(a, b)$. Poiché esistono $r, s \in \mathbb{Z}$ tali che $MCD(a, b) = ar + bs$ abbiamo anche che $c = a(qr) + b(qs)$, e quindi l' equazione ha soluzioni.

Vogliamo ora trovare tutte le soluzioni dell' equazione. D' altra parte, qualunque sia $h \in \mathbb{Z}$ abbiamo $a\frac{bh}{MCD(a,b)} + b\left(-\frac{ah}{MCD(a,b)}\right) = 0$, e quindi

$$c = a\left(qr + \frac{bh}{MCD(a, b)}\right) + b\left(qs - \frac{ah}{MCD(a, b)}\right)$$

qualunque sia $h \in \mathbb{Z}$ e quindi $S = \{\left(qr + \frac{bh}{MCD(a,b)}, qs - \frac{ah}{MCD(a,b)}\right) | h \in \mathbb{Z}\}$ è un insieme di soluzioni dell' equazione data. Verifichiamo che non ce ne sono altre. Sia (x_0, y_0) una soluzione. Allora $c = ax_0 + by_0 = aqr + bqs$. Sottraendo abbiamo $a(x_0 - qr) + b(y_0 - qs) = 0$ e quindi $(x_0 - qr, y_0 - qs)$ è soluzione dell' equazione omogenea $aX + bY = 0$. Dividendo per $MCD(a, b)$ abbiamo l' equazione

$$\frac{a}{MCD(a, b)}X + \frac{b}{MCD(a, b)}Y = 0$$

con $MCD(\frac{a}{MCD(a,b)}, \frac{b}{MCD(a,b)}) = 1$. Poiché $\frac{a}{MCD(a,b)}$ divide $-\frac{b}{MCD(a,b)}Y$ ma non ha primi in comune con $\frac{b}{MCD(a,b)}$ allora esso divide Y, e quindi $Y = -\frac{a}{MCD(a,b)}h$ per qualche $h \in \mathbb{Z}$. Sostituendo e dividendo per $\frac{a}{MCD(a,b)}$ abbiamo $X = \frac{b}{MCD(a,b)}h$ e quindi $(x_0, y_0) \in S$. □

Analogamente, si può dimostrare che

Proposizione 13. *L' equazione $ax + by + cz = d$ con $a, b, c, d \in \mathbb{Z}$ ha soluzioni se, e solo se, $MCD(a, b, c)|d$. In questo caso, ha infinite soluzioni che dipendono da due parametri liberi in $\mathbb{Z}$.*

Non dimostriamo la precedente Proposizione, ma diamo la forma delle soluzioni. Assumiamo che l' equazione abbia soluzioni, e che $MCD(a,b,c) = 1$. Detti r, s interi che verificano $ar + MCD(b,c)s = 1$, e detti r', s' interi che verificano $br' + cs' = MCD(b,c)$ allora le soluzioni sono tutte e sole quelle della forma $(rd - MCD(b,c)h, r'sd + r'ah - \frac{c}{MCD(b,c)}k, ss'd + as'h + \frac{b}{MCD(b,c)}k)$ con $h, k \in \mathbb{Z}$.

Ovviamente, le Proposizioni precedenti possono essere generalizzate ad un' equazione lineare in un numero arbitrario di incognite. Inoltre, risolvendo un' equazione alla volta, è possibile trovare le soluzioni intere anche di un sistema lineare a coefficienti interi.

Esempio 14. Troviamo ad esempio le soluzioni intere dell' equazione $8x + 6y = 8$.

Poiché $MCD(8,6) = 2$ divide 8 termine noto dell' equazione, l' equazione ha soluzioni. Osserviamo che $8 \cdot 1 + 6 \cdot (-1) = MCD(8,6)$. Quindi, in accordo alla formula trovata, le soluzioni sono tutte e sole quelle della forma $(4 + 3h, -4 - 4h)$, con $h \in \mathbb{Z}$.

Esempio 15. Risolvere in $\mathbb{Z}$, se possibile, il sistema lineare

$$\begin{cases} 2x + 5y = -4 \\ 3x + 2y = 5 \end{cases}$$

Risolviamo la prima equazione, usando il metodo precedentemente esposto. Essa ha soluzioni perché $MCD(2,5) = 1$, ed esse sono tutte e sole quelle della forma $(8+5h, -4-2h)$ con $h \in \mathbb{Z}$. Sostituendo nella seconda equazione, otteniamo la nuova equazione $3(8+5h)+2(-4-2h) = 5$ ossia $11h = -11$ nell' incognita h. Essa ha l' unica soluzione $h = -1$, e quindi l' unica soluzione del sistema dato è $(8-5, -4+2) = (3, -2)$.

Riprendiamo ora la divisione tra interi. Fissiamo $a \in \mathbb{N}, a \neq 0$. I possibili resti della divisione per a sono $0, 1, \ldots, a-1$, ed è ovvio che tutti vengono realizzati. Non solo, ma possiamo ripartire gli interi in base al resto che si ottiene nella divisione per a, ottenendo le cosiddette classi dei resti. Infatti, abbiamo

Lemma 16. *Sia $a \in \mathbb{N}$ un intero non nullo, e sia r un possibile resto, ossia $0 \leq r < a$. Tutti e soli gli interi che divisi per a hanno resto r sono quelli dell' insieme*

$$[r]_a = \{r + ah | h \in \mathbb{Z}\}.$$

Dimostrazione. È evidente che ogni elemento di $[r]_a$ ha resto r nella divisione per a, dalla definizione di quoziente e resto. Sia $c \in \mathbb{Z}$ un intero che ha resto r nella divisione per a. Allora $c = qa + r$, e quindi $c \in [r]_a$ per $h = q$. □

Per convenzione, se $b \in \mathbb{Z}$ poniamo $[b]_a = [r]_a$ dove r è il resto della divisione di b per a.

Infine, è chiaro che $\mathbb{Z} = [0]_a \cup [1]_a \cup \cdots \cup [a-1]_a$ e che $[r]_a \cap [r']_a \neq \emptyset$ se, e solo se, r ed r' hanno lo stesso resto nella divisione per a.

Definizione 17. *Sia $a \in \mathbb{N}$ un intero non nullo. L' insieme delle classi dei resti nella divisione per a si indica con $\mathbb{Z}_a$, ossia $\mathbb{Z}_a = \{[0]_a, [1]_a, \ldots, [a-1]_a\}$.*

Vogliamo ora definire l' operazione di somma e di prodotto tra gli elementi di $\mathbb{Z}_a$.

Cominciamo con la seguente osservazione.

Lemma 18. *Siano $b \in [r]_a$ e $c \in [r']_a$ due interi. Allora $b + c$ ed $r + r'$ hanno lo stesso resto nella divisione per a.*

Dimostrazione. Dalla definizione delle classi dei resti, abbiamo che $b = ha + r, c = ka + r'$. Sommando abbiamo $b + c = (h + k)a + r + r'$. Se $r + r' = qa + r''$ allora $b + c = (h + k + q)a + r''$ e questo prova l' asserto. □

Il Lemma precedente permette allora di definire la somma di due classi come la classe del resto della somma di due elementi qualsiasi nella classe, ossia

Definizione 19. *In $\mathbb{Z}_a$ definiamo la somma come*

$$[r]_a + [r']_a = [r + r']_a$$

qualunque siano le classi $[r]_a$ ed $[r']_a$.

La somma verifica le stesse proprietà della somma di interi, ossia è associativa, commutativa, la classe $[0]_a$ è elemento neutro, ossia $[r]_a + [0]_a = [r]_a$ per ogni $[r]_a \in \mathbb{Z}_a$, ed ogni classe ha l' opposto perché $[r]_a + [a - r]_a = [0]_a$.

Prima di definire il prodotto di due classi osserviamo la seguente proprietà .

Lemma 20. *Siano $b \in [r]_a, c \in [r']_a$. Allora bc ed rr' hanno lo stesso resto nella divisione per a.*

Dimostrazione. Dalla definizione delle classi dei resti abbiamo che $b = ha+r, c = ka+r'$. Quindi $bc = (hka + kr + hr')a + rr'$. Se $rr' = qa + r''$ allora $bc = (hka + kr + hr' + q)a + r''$ e quindi bc ed rr' hanno lo stesso resto nella divisione per a. □

Possiamo allora definire il prodotto di due classi come la classe del prodotto di due elementi qualsiasi nelle classi, ossia

Definizione 21. *Siano $[r]_a, [r']_a \in \mathbb{Z}_a$ due classi di resti. Allora*

$$[r]_a[r']_a = [rr']_a.$$

Anche il prodotto ha regole di calcolo simili a quelle del prodotto di interi. Infatti, il prodotto è associativo, commutativo, la classe $[1]_a$ è elemento neutro del prodotto, ossia $[r]_a[1]_a = [r]_a$ qualunque sia $[r]_a \in \mathbb{Z}_a$. Inoltre, vale la proprietà distributiva del prodotto rispetto alla somma.

A differenza del prodotto in $\mathbb{Z}$, possono esistere altri elementi oltre alla classe $[1]_a$ che hanno inverso moltiplicativo. Non solo, ma possono esistere anche elementi non nulli che moltiplicati tra loro danno $[0]_a$ come risultato.

Esempio 22. Calcoliamo i prodotti $[3]_8[3]_8$, ed $[4]_8[6]_8$.

Dalla definizione otteniamo $[3]_8[3]_8 = [3 \cdot 3]_8 = [9]_8 = [1]_8$ e quindi $[3]_8$ è l' inverso moltiplicativo di se stesso. Sempre dalla definizione otteniamo che $[4]_8[6]_8 = [4 \cdot 6]_8 = [24]_8 = [0]_8$ e quindi possiamo affermare che in $\mathbb{Z}_8$ non vale la legge di annullamento del prodotto.

Per fissare la terminologia, diamo la definizione seguente.

Definizione 23. *$[r]_a$ è invertibile se esiste $[s]_a$ tale che $[r]_a[s]_a = [1]_a$. $[r]_a$ è divisore dello zero se esiste $[s]_a \neq [0]_a$ tale che $[r]_a[s]_a = [0]_a$.*

Caratterizziamo ora gli elementi invertibili ed i divisori dello zero in $\mathbb{Z}_a$.

Teorema 24. *$[r]_a$ è invertibile in $\mathbb{Z}_a$ se, e solo se, $MCD(r, a) = 1$. $[r]_a$ è un divisore dello zero in $\mathbb{Z}_a$ se, e solo se, $MCD(a, r) \neq 1$.*

Dimostrazione. Se $[r]_a$ è invertibile allora esiste $[s]_a$ tale che $[r]_a[s]_a = [1]_a$ per definizione di elemento invertibile. Per come definito il prodotto, abbiamo che $[rs]_a = [1]_a$ ossia rs ha resto 1 se diviso per a. Quindi $rs = qa + 1$ ossia $rs - qa = 1$. L' uguaglianza precedente vuol dire che l' equazione $rx + ay = 1$ ha soluzioni, ma questo può capitare se, e solo se, $MCD(r, a)$ divide il termine noto 1, ossia se, e solo se, $MCD(r, a) = 1$. Viceversa, se $MCD(r, a) = 1$ allora l' equazione $rx + ay = 1$ ha soluzioni e quindi $[r]_a$ è invertibile.

Supponiamo ora che $[r]_a$ sia un divisore dello zero. Quindi esiste $[s]_a \neq [0]_a$ tale che $[r]_a[s]_a = [0]_a$. Per come definito il prodotto, abbiamo che $[rs]_a = [0]_a$ ossia $rs = qa$. Se $MCD(r,a) = 1$ allora a divide s e quindi $[s]_a = [0]_a$, ma questo è escluso. Quindi $MCD(r,a) \neq 1$. Viceversa, se $MCD(r,a) \neq 1$, allora $[r]_a \left[\frac{a}{MCD(r,a)}\right]_a = [mcm(r,a)]_a = [0]_a$ perché a divide $mcm(r,a)$. Essendo $\frac{a}{MCD(r,a)}$ non divisibile per a allora $[r]_a$ è un divisore dello zero. □

Dal Teorema segue immediatamente che

Corollario 25. *Tutti gli elementi non nulli di $\mathbb{Z}_a$ sono invertibili se, e solo se, a è un numero primo.*

In ultimo, vogliamo risolvere equazioni lineari in una incognita in $\mathbb{Z}_a$, dette equazioni congruenziali. Una tale equazione si presenta nella forma $[r]_a[x]_a = [b]_a$ oppure nella forma equivalente $rx = b \mod a$. Per come definite le operazioni in $\mathbb{Z}_a$, l' equazione precedente è equivalente all' equazione $rx + ay = b$. In particolare, l' equazione congruenziale data ha soluzioni se, e solo se, $MCD(r,a)$ divide b. Le sue soluzioni si ricavano poi da quelli dell' equazione in due variabili, come si può vedere dal seguente esempio.

Esempio 26. Risolvere l' equazione $6x = 2 \mod 8$.

L' equazione data è equivalente all' equazione $6x + 8y = 2$. Poiché $MCD(6,8) = 2$ l' equazione ha soluzioni. Dalla formula spiegata precedentemente otteniamo che le soluzioni sono tutte e sole quelle della forma $(-1 + 4h, 1 - 3h)$ con $h \in \mathbb{Z}$. Quindi, le soluzioni dell' equazione congruenziale sono le classi $[-1 + 4h]_8$ con $h \in \mathbb{Z}$. Per h pari, ossia $h = 2k$ i numeri $-1 + 8k$ hanno resto 7 nella divisione per 8. Per h dispari, ossia $h = 2k + 1$, i numeri $3 + 8k$ hanno resto 3 nella divisione per 8. Quindi, le soluzioni sono $[3]_8, [7]_8$. Esplicitamente osserviamo che equazioni di primo grado in una incognita in $\mathbb{Z}_a$ possono avere anche più soluzioni.

Ricordiamo ora alcuni cambiamenti relativi al modo con cui si lavora con le matrici ad entrate in $\mathbb{Z}_a$.

Teorema 27. *Sia A una matrice quadrata ad entrate in $\mathbb{Z}_a$. A è invertibile se, e solo se,* $\det(A)$ *è invertibile in $\mathbb{Z}_a$.*

Nella riduzione di matrici, invece, le operazioni elementari effettuabili sono

(1) scambio di righe: $R_i \leftrightarrow R_j$;
(2) prodotto di una riga per un elemento invertibile: $R_i \to [r]_a R_i$ con $[r]_a$ invertibile;
(3) combinazione di una riga per un multiplo di un' altra: $R_h \to R_h + [r]_a R_i$ con $i \neq h$.

Osservazione 28. Esistono matrici quadrate di rango massimo che non sono invertibili. Ad esempio, la matrice

$$A = \begin{pmatrix} 2 & 4 \\ 0 & 2 \end{pmatrix}$$

è ridotta di rango 2 ma non invertibile in $\mathbb{Z}_6$.

2. Esercizi

Esercizio 29. Scrivere quoziente e resto della divisione delle seguenti coppie di interi:

(1) $152, 13$;
(2) $134, 21$;
(3) $-73, 14$.

Esercizio 30. Trovare il massimo comun divisore, sia con la decomposizione in primi, sia col metodo di Euclide, ed il minimo comune multiplo delle seguenti coppie di interi:

(1) $16, 24$;
(2) $27, 45$;
(3) $55, 121$.

Esercizio 31. Per le coppie di interi (a, b) del precedente Esercizio 30, trovare gli interi r, s in modo che

$$MCD(a, b) = ra + sb.$$

Esercizio 32. Dire, per le coppie di interi degli Esercizi 29, 30, a quale classe di resti modulo b corrisponde il numero a.

Esercizio 33. Elencare gli elementi di $\mathbb{Z}_6$ e calcolare le tavole della somma e del prodotto. Quali sono gli elementi invertibili?

Esercizio 34. Trovare, se possibile, tutte le soluzioni intere delle seguenti equazioni:

(1) $4x + 6y = 0$;
(2) $12x - 18y = -6$;
(3) $12x + 10y = 3$.

Trovare poi le eventuali soluzioni comuni alle prime due equazioni.

Esercizio 35. Risolvere le seguenti equazioni congruenziali:

(1) $4x = 3 \mod 5$;
(2) $4x = 5 \mod 9$;
(3) $6x = 3 \mod 35$.

Esercizio 36. Calcolare il rango della matrice

$$A = \begin{pmatrix} 2 & 4 & 1 \\ 4 & 2 & 5 \end{pmatrix}$$

i cui elementi sono in $\mathbb{Z}_6$, oppure in $\mathbb{Z}_3$, oppure in $\mathbb{Z}_4$.

Esercizio 37. Discutere il sistema lineare a coefficienti in $\mathbb{Z}_3$ al variare di $a \in \mathbb{Z}_3$

$$\begin{cases} x + y + z = 1 \\ x + az = 2 \\ 2x + z = 2a. \end{cases}$$

Posto poi $a = 1$ calcolare le soluzioni del sistema sia con il metodo di riduzione, sia con quello di Cramer, se possibile.

Esercizio 38. Calcolare se possibile l' inversa della matrice

$$A = \begin{pmatrix} 2 & 1 \\ 2 & 5 \end{pmatrix}$$

sia in $\mathbb{Z}_4$, sia in $\mathbb{Z}_5$, sia in $\mathbb{Z}_6$.

Esercizio 39. Il prodotto $5 \cdot 4 = 0$ in

(1) $\mathbb{Z}_6$;
(2) $\mathbb{Z}_{10}$;
(3) $\mathbb{Z}_8$;
(4) $\mathbb{Z}_{12}$.

Esercizio 40. La matrice

$$A = \begin{pmatrix} 1 & -3 \\ 3 & 3 \end{pmatrix}$$

è invertibile in

(1) $\mathbb{Z}_3$;
(2) $\mathbb{Z}_4$;
(3) $\mathbb{Z}_5$;
(4) $\mathbb{Z}_6$.

Esercizio 41. La soluzione dell' equazione $7x = 3 \mod 8$ è

(1) 1;
(2) 3;
(3) 5;
(4) 7.

3. Soluzioni di alcuni esercizi

Soluzione dell' Esercizio 29. Ricordiamo che il quoziente q ed il resto r della divisione di a per b con a, b interi sono due interi tali che

(1) $a = qb + r$;
(2) $0 \leq r < |b|$.

Per la prima coppia di interi, $a = 152$ e $b = 13$. Effettuando la divisione, abbiamo

$$152 = 11 \cdot 13 + 9$$

e quindi $q = 11, r = 9$.

Per la seconda coppia, abbiamo $a = 134, b = 21$, e

$$134 = 6 \cdot 21 + 8.$$

Quindi $q = 6, r = 8$.

Per la terza ed ultima coppia, abbiamo $a = -73, b = 14$ ed inoltre

$$-73 = -6 \cdot 14 + 11.$$

Quindi, $q = -6, r = 11$.

Soluzione dell' Esercizio 30. Analizziamo la prima coppia $(a, b) = (16, 24)$. Utilizzando la decomposizione in primi abbiamo $16 = 2^4, 24 = 2^3 \cdot 3$, e quindi $MCD(16, 24) = 2^3 = 8$. Usando il metodo di Euclide, abbiamo la seguente successione di divisioni:

(1) $24 = 1 \cdot 16 + 8$,
(2) $16 = 2 \cdot 8 + 0$.

La successione si arresta quando il resto è uguale a 0, e l' ultimo divisore è il massimo comun divisore cercato. Quindi anche con questo metodo abbiamo $MCD(a, b) = 8$.

Il minimo comune multiplo di $(16, 24)$ è uguale a

$$mcm(16, 24) = \frac{16 \cdot 24}{MCD(16, 24)} = 48 = 2^4 \cdot 3.$$

La seconda coppia è $(a, b) = (27, 45)$. Procedendo come nel caso precedente, abbiamo $27 = 3^3, 45 = 3^2 \cdot 5$, e quindi

$$MCD(27, 45) = 3^2 = 9.$$

Usando l' algoritmo di Euclide, abbiamo

(1) $45 = 1 \cdot 27 + 18$,

(2) $27 = 1 \cdot 18 + 9$,
(3) $18 = 2 \cdot 9 + 0$,

e quindi $MCD(27, 45) = 9$.

Il minimo comune multiplo è uguale a $mcm(27, 45) = 3^3 \cdot 5 = 135$.

L' ultima coppia è $(a, b) = (55, 121)$. Abbiamo che $55 = 5 \cdot 11, 121 = 11^2$ e quindi $MCD(55, 121) = 11$. Con l' algoritmo di Euclide, abbiamo invece

(1) $121 = 2 \cdot 55 + 11$,
(2) $55 = 5 \cdot 11 + 0$,

e quindi $MCD(55, 121) = 11$.

Il loro minimo comune multiplo è uguale a $mcm(55, 121) = 11^2 \cdot 5 = 605$.

Soluzione dell' Esercizio 31. Seguiamo le divisioni effettuate nell' algoritmo di Euclide, ed otteniamo gli interi r, s cercati.

Per la prima coppia, dobbiamo cercare r, s tali che $8 = r \cdot 24 + s \cdot 16$. Quindi abbiamo che la seconda ed ultima divisione conferma che 8 è il massimo comun divisore di $16, 24$, e la prima, fornisce $8 = 1 \cdot 24 - 1 \cdot 16$. Quindi $r = 1$, mentre $s = -1$.

Per la seconda coppia, dobbiamo cercare gli interi r, s in modo che $9 = r \cdot 27 + s \cdot 45$. Seguendo le divisioni, abbiamo che la terza conferma che 9 è il massimo comun divisore di 27 e 45, la seconda che $9 = 1 \cdot 27 - 1 \cdot 18$, e la prima che $18 = 1 \cdot 45 - 1 \cdot 27$. Sostituendo l' espressione che calcola 18, otteniamo

$$9 = 1 \cdot 27 - 1 \cdot (1 \cdot 45 - 1 \cdot 27) = 2 \cdot 27 - 1 \cdot 45.$$

Quindi, $r = 2, s = -1$.

Per la terza coppia, è immediato, dalla prima divisione, che $11 = 1 \cdot 121 - 2 \cdot 55$.

Soluzione dell' Esercizio 32. Bisogna calcolare il resto della divisione di a per b. Quindi abbiamo

(1) $152 = 11 \cdot 13 + 9$, da cui $152 = 9 \mod 13$;
(2) $134 = 6 \cdot 21 + 8$, da cui $134 = 8 \mod 21$;
(3) $-73 = -6 \cdot 14 + 11$, da cui $-73 = 11 \mod 14$;
(4) $16 = 0 \cdot 24 + 16$, da cui $16 = 16 \mod 24$;
(5) $27 = 0 \cdot 45 + 27$, da cui $27 = 27 \mod 45$;
(6) $55 = 0 \cdot 121 + 55$, da cui $55 = 55 \mod 121$.

Soluzione dell' Esercizio 33. Gli elementi di $\mathbb{Z}_6$ sono tutti e soli i possibili resti della divisione per 6, e quindi

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}.$$

Per quanto riguarda le tavole della somma e del prodotto, esse sono

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
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

Gli unici elementi invertbili sono 1 e 5 ed i loro inversi sono 1 e 5, rispettivamente.

Soluzione dell' Esercizio 34. Il massimo comun divisore dei coefficienti della prima equazio- ne è 2. Semplificandolo, otteniamo l' equazione $2x + 3y = 0$. È ovvio che $(3, -2)$ è una soluzione, e che anche $(3a, -2a)$ è una soluzione, qualunque sia $a \in \mathbb{Z}$. Sia (r, s) una soluzione. Allora,$2r = -3s$, e quindi 2 divide s, ossia $s = -2b$, per qualche $b \in \mathbb{Z}$. So- stituendo, otteniamo $2r = 6b$, ossia $r = 3b$, e quindi tutte e sole le soluzioni sono della forma $(3a, -2a)$ con $a \in \mathbb{Z}$.

La seconda equazione ha soluzioni perché il termine noto è un multiplo del massimo comun divisore dei coefficienti delle incognite (condizione necessaria e sufficiente perché l' equazione abbia soluzioni). Dopo aver semplificato il massimo comun divisore, l' equazione diventa $2x-3y = -1$. Una soluzione particolare dell' equazione è $(1, 1)$, mentre le soluzioni dell' equazione omogenea associata sono $(3b, 2b)$ al variare di $b \in \mathbb{Z}$. Quindi, tutte e sole le soluzioni sono della forma $(3b + 1, 2b + 1)$, con $b \in \mathbb{Z}$.

La terza equazione non ha soluzioni perché il massimo comun divisore dei coefficienti delle incognite è 2 ed il termine noto non è divisibile per 2.

Le soluzioni comuni alle prime due equazioni si possono ricavare dall' uguaglianza $(3a, -2a) = (3b + 1, 2b + 1)$. Si ottiene allora il sistema

$$\begin{cases} 3a - 3b = 1 \\ -2a - 2b = 1. \end{cases}$$

Tale sistema non ha soluzioni perché il termine noto della prima equazione non è divisibile per 3 che è il massimo comun divisore dei coefficienti delle incognite dell' equazione in oggetto. Non avendo la prima equazione soluzioni, tutto il sistema non ha soluzioni.

Soluzione dell' Esercizio 35. Ricordiamo che un elemento a è invertibile $\mod b$ se, e solo se, $MCD(a, b) = 1$.

Consideriamo la prima equazione. $MCD(4, 5) = 1$ e quindi 4 è invertibile $\mod 5$. Il suo inverso è 4 perché $4 \cdot 4 = 16 = 3 \cdot 5 + 1$. La soluzione della prima equazione è allora $x = 4 \cdot 3 \mod 5 = 2 \mod 5$, ottenuta moltiplicando entrambi i membri dell' equazione per l' inverso del coefficiente della x.

Per la seconda equazione abbiamo $MCD(4, 9) = 1$, e quindi 4 è invertibile anche $\mod 9$. Il suo inverso è 7 perché $4 \cdot 7 = 28 = 3 \cdot 9 + 1$. La soluzione dell' equazione si ottiene moltiplicano ambo i membri per 7 ed è $x = 5 \cdot 7 = 35 = 8 \mod 9$.

Per la terza equazione, abbiamo che $MCD(6, 35) = 1$, e l' inverso di 6 è uguale a 6 $\mod 35$. Moltiplicando ambo i membri per 6 otteniamo $x = 6 \cdot 3 = 18 \mod 35$.

Soluzione dell' Esercizio 36. In $\mathbb{Z}_6$, l' unico elemento invertibile della prima riga è 1. Per ridurre la matrice, effettuiamo allora l' operazione elementare $R_2 \to R_2 + R_1$ ed otteniamo la matrice

$$\begin{pmatrix} 2 & 4 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

e quindi il rango di A è uguale a 1.

In $\mathbb{Z}_3$ la matrice A diventa

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix}.$$

Effettuando l' operazione elementare $R_2 \to R_2 + 2R_1$ otteniamo la matrice

$$\begin{pmatrix} 2 & 1 & 1 \\ 2 & 1 & 0 \end{pmatrix}$$

e quindi la matrice A ha rango 2.

In $\mathbb{Z}_4$, la matrice A diventa

$$A = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix},$$

che ha rango 2 essendo già ridotta.

Soluzione dell' Esercizio 37. La matrice completa del sistema è

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 0 & a & 2 \\ 2 & 0 & 1 & 2a \end{array}\right).$$

Effettuando l' operazione elementare $R_3 \to R_3 + R_2$ otteniamo la matrice

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 0 & a & 2 \\ 0 & 0 & 1+a & 2a+2 \end{array}\right).$$

Il rango della matrice dei coefficienti è 3 se $1 + a \neq 0$, ossia se $a \neq 2$, mentre è uguale a 2 se $a = 2$. Il rango della matrice completa è uguale a 2 se $a = 2$, ed è uguale a 3 se $a \neq 2$. Quindi i ranghi delle due matrici sono sempre uguali, ed il sistema ha una sola soluzione se $a \neq 2$, mentre ha soluzioni che dipendono da un parametro libero se $a = 2$.

Posto $a = 1$ nella matrice ridotta, otteniamo l' unica soluzione del sistema che è uguale a $(0, 2, 2)$. Per $a = 1$, la matrice dei coefficienti del sistema è invertibile, e la sua inversa è

$$A^{-1} = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 2 & 0 \\ 0 & 2 & 2 \end{pmatrix}$$

e quindi, con il metodo di Cramer, la soluzione si calcola come $X = A^{-1}B$ essendo B la colona dei termini noti. Ovviamente, si riottiene la stessa soluzione.

Soluzione dell' Esercizio 38. Una matrice quadrata è invertibile se, e solo se, il suo determinante è invertibile. Il deteminante di A è uguale a $\det(A) = 8$, che è invertibile solo in $\mathbb{Z}_5$ tra le tre possibilità date. In particolare, l' inverso di 8 è 2 mod 5. L' inversa di A si calcola o risolvendo il sistema $AX = I$ o con i complementi algebrici. In entrambi i casi si ottiene la matrice

$$A^{-1} = \begin{pmatrix} 0 & 3 \\ 1 & 4 \end{pmatrix}.$$

Soluzione dell' Esercizio 39. Se l' uguaglianza è vera, allora 20 è divisibile per la base in cui effettuiamo i calcoli. L' unica risposta vera è quindi $\mathbb{Z}_{10}$ da cui la (2) è vera.

Soluzione dell' Esercizio 40. La matrice è invertibile se il suo deteminante è invertibile. Poiché $\det(A) = 12$, otteniamo che A è invertibile solo in $\mathbb{Z}_5$. Quindi, (3) è l' unica risposta vera.

Soluzione dell' Esercizio 41. 7 è invertibile mod 8 ed il suo inverso è 7. La soluzione è allora $x = 7 \cdot 3 = 21 = 5$ mod 8. Quindi, (3) è l' unica risposta vera.