Capitolo 3

Il campo $\mathbb{Z}_n$

3.1 Introduzione

Introduciamo ora un altro campo, formato da un numero finito di elementi; il campo delle classi resto modulo n, con n numero primo.

3.2 Le classi resto

Definizione 3.1 Dato un insieme finito G con un'oprazione che indichiamo con il simbolo $*$, possiamo considerare la **tabella dell'operazione** di G. Per far ciò indichiamo con $a_1, a_2, \ldots, a_n$ gli elementi di G. La tabella dell'operazione di G è la matrice quadrata di ordine n tale che al posto i, j vi è l'elemento $a_i * a_j$. Per rendere più esplicito il tutto si scrivono a lato gli elementi. Si ha quindi una tabella così fatta:

	a_1	a_2	$\ldots$	a_j	$\ldots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$\ldots$	$a_1 * a_j$	$\ldots$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\ldots$	$a_2 * a_j$	$\ldots$	$a_2 * a_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_i	$a_i * a_1$	$a_i * a_2$	$\ldots$	$a_i * a_j$	$\ldots$	$a_i * a_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_n	$a_n * a_1$	$a_n * a_2$	$\ldots$	$a_n * a_j$	$\ldots$	$a_n * a_n$

Esempio 3.2 Nell'insieme $K = \{P, D\}$ abbiamo introdotto l'operazione di moltiplicazione:

$$P \cdot P = P \ , \ P \cdot D = P \ , \ D \cdot P = P \ , \ D \cdot D = D$$

La tabella della moltiplicazione è:

	P	D
P	P	P
D	P	D

In modo analogo si può scrivere (esercizio) la tabella dell'addizione.

Abbiamo già ricordato che le operazioni che abbiamo dato derivano dal fatto che abbiamo pensato P come l'insieme di tutti i numeri pari e D come l'insieme di tutti i numeri dispari.

Naturalmente i numeri pari possono essere definiti come i numeri che, divisi per 2, hanno come resto 0. I numeri dispari sono invece i numeri che, divisi per 2, hanno come resto 1. △

Vogliamo ora generalizzare tutto ciò.

Per poter generalizzare dobbiamo richiamare alcune nozioni di aritmetica. Sia fissato un numero $n \in \mathbb{N}^* = \mathbb{N} - \{0\}$. Quindi n è un numero intero positivo. Sappiamo che, dato comunque un numero $a \in \mathbb{N}$, possiamo dividere a per n e ottenere un numero intero q (quoziente) con resto un numero intero positivo o nullo r minore di n. Sappiamo ciò fin dalle scuole elementari. Dato quindi $a \in \mathbb{Z}$ con ≥ 0, sappiamo determinare due numeri interi q e r tali che si abbia:

$$a = qn + r$$

Notiamo che si ha $0 \leq r < n$.
Vogliamo generalizzare tutto ciò al caso di un numero a intero, sia esso positivo, negativo o nullo.
Ricordiamo che con il simboli $\mathbb{Z}$ indichiamo i numeri interi, positivi, negativi o nulli.

Abbiamo il seguente teorema.

Teorema 3.3 *Sia fissato $n \in \mathbb{N}^*$. Dato $a \in \mathbb{Z}$, esistono e sono unici i numeri $q \in \mathbb{Z}$ e $r \in \mathbb{Z}$ tali che:*

$$a = qn + r \quad \text{con} \quad 0 \leq r < n$$

Dimostrazione Nel caso in cui $a \geq 0$ sappiamo come fare.
Studiamo ora il caso in cui si abbia $a < 0$. Consideriamo $-a$. Si ha $-a > 0$. Applichiamo a $-a$ l'algoritmo appena detto. Otteniamo $-a = q'n + r'$ con $q' \in \mathbb{Z}$ e $r' \in \mathbb{Z}$ tale che $0 \leq r' < n$. Abbiamo allora $a = -q'n + (-r')$ con $-n < -r' \leq 0$. Distinguiamo due casi. Se $r' = 0$ abbiamo $a = qn+r$ con $q = -q'$ e $r = 0$. Se $r' > 0$ abbiamo $a = -q'n - n + (n - r') = (-q' - 1)n + (n - r')$ con $0 < n - r' < n$. Abbiamo perciò $a = qn + r$ con $q = -q' - 1$ e $r = n - r'$.
Bene, per ogni $a \in \mathbb{Z}$ abbiamo ora un algoritmo per determinare i numeri q e r verificanti le condizioni richieste.
Dobbiamo ora dimostrare che r e q sono unici. Si abbia:
$a = qn + r$ con $q \in \mathbb{Z}$ e $0 \leq r < n$ e si abbia anche:

$a = q'n + r'$ con $q' \in \mathbb{Z}$ e $0 \leq r' < n$.
Sia $r' \geq r$. Allora $0 \leq r' - r = (q - q')n \leq r' < n$. Da cui $0 \leq (q - q')n < n$. Da ciò segue $0 \leq q - q' < 1$. Ma allora, essendo $q - q'$ un intero positivo o nullo, si ha $q - q' = 0$; da cui $q = q'$ e $r = r'$. Cioè la tesi. ■

Esempio 3.4 Per rendere più chiaro l'algoritmo facciamo un esempio. Prendiamo $a = -1223$ e $b = 14$.
Consideriamo il numero 1223 e dividiamolo per 14. Utilizzando una qualsiasi calcolatrice tascabile otteniamo $1223/14 = 87,35...$ Abbiamo perciò $q' = 87$. Si ha poi $r' = 1223 - 87 \cdot 14 = 1223 - 1218 = 5$.
Abbiamo pertanto:

$$1223 = 87 \cdot 14 + 5$$

Ne segue:

$$-1223 = -87 \cdot 14 - 5 = -87 \cdot 14 - 14 + 14 - 5 = -88 \cdot 14 + 9$$

I nostri q e r cercati sono quindi rispettivamente -88 e 9. △

Definizione 3.5 Sia $n \in \mathbb{N}^*$. Poniamo in $\mathbb{Z}$ la seguente relazione:

$$a \sim a' \Longleftrightarrow a - a' = q \cdot n \text{ con } q \in \mathbb{Z}.$$

Quindi $a \sim a'$ se e solo se $a - a'$ è un multiplo di n. Usiamo il seguente simbolismo:
se $a \sim b$ scriviamo $a \equiv b \pmod{n}$ e diciamo a **congruo** b **modulo** n. La relazione si dice **relazione di congruenza modulo** n. △

Teorema 3.6 *La relazione di congruenza modulo n è una relazione di equivalenza.*

Dimostrazione Dobbiamo dimostrare che sono valide le proprietà riflessiva, simmetrica e transitiva.
(a) proprietà riflessiva:
$a \equiv a \pmod{n} \quad \forall a \in \mathbb{Z}$.
Infatti $a - a = 0 = 0n$.
(b) proprietà simmetrica:
$a \equiv b \pmod{n} \Longrightarrow b \equiv a \pmod{n}$.
Infatti:
$a \equiv b \pmod{n} \Longrightarrow a - b = qn \ , \ q \in \mathbb{Z} \Longrightarrow$
$\Longrightarrow b - a = -qn, -q \in \mathbb{Z} \Longrightarrow b \equiv a \pmod{n}$.
(c) proprietà transitiva:
$a \equiv b \pmod{n} \ , \ b \equiv c \pmod{n} \Longrightarrow a \equiv c \pmod{n}$.
Infatti da:
$a \equiv b \pmod{n} \ , \ b \equiv c \pmod{n}$
segue:
$a - b = hn \ , \ b - c = kn \quad \text{con} \quad h \in \mathbb{Z} \ , \ k \in \mathbb{Z}$.
E quindi:
$a - c = a - b + b - c = hn + kn = (h + k)n \ , \ h + k \in \mathbb{Z} \Longrightarrow a \equiv c \pmod{n}$.
Cioè la tesi. □ ■

Definizione 3.7 Fissato un numero n intero positivo, consideriamo in $\mathbb{Z}$ la relazione di equivalenza della congruenza modulo n.
Dato $a \in \mathbb{Z}$ indichiamo con $[a]_n$ l'insieme dei numeri b congrui ad a modulo n. Essa viene chiamata **classe di congruenza modulo n determinata da a**. Si ha quindi (esercizio):

$$[a]_n = \{a + hn \ , \ h \in \mathbb{Z}\}$$

Osserviamo (vedi nota successiva) che ogni numero $a \in \mathbb{Z}$ appartiene ad una ed una sola classe di congruenza modulo n. Indichiamo con $\mathbb{Z}_n$ l'insieme di tutte le classi di congruenza modulo n. △

Nota 3.8 Il fatto che un numero appartiene ad una sola classe di congruenza deriva dal fatto che se due classi hanno intersezione non vuota, allora le due classi coincidono. Per dimostrare ciò supponiamo di avere due classi $[a]_n$ e $[b]_n$ per le quali esista un numero c tale che $c \in [a]_n$ e $c \in [b]_n$. Dobbiamo dimostrare che si ha $[a]_n = [b]_n$. Dobbiamo quindi dimostrare che se $d \in [a]_n$ allora $d \in [b]_n$ e viceversa.
Poiché $d \in [a]_n$, si ha $d \equiv a \pmod{n}$. Poiché $c \in [a]_n$ allora $c \equiv a \pmod{n}$ e quindi $a \equiv c \pmod{n}$. D'altronde da $c \in [b]_n$ segue $c \equiv b \pmod{n}$. Ma allora da $d \equiv a \pmod{n}$, $a \equiv c \pmod{n}$, $c \equiv b \pmod{n}$ segue $d \equiv b \pmod{n}$, per la proprietà transitiva. Cioè $d \in [b]_n$. Il viceversa si dimostra in modo analogo. △

Esempio 3.9 Si consideri $n = 2$. Si ha:
$[0]_2 = \{0 + 2h \ , \ h \in \mathbb{Z}\}$. Essa è quindi l'insieme dei numeri pari.
$[1]_2 = \{1 + 2h \ , \ h \in \mathbb{Z}\}$. Essa è quindi l'insieme dei numeri dispari.
Si ha perciò $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. △

Esempio 3.10 Si consideri $n = 3$. Si ha:
$[0]_3 = \{0 + 3h \ , \ h \in \mathbb{Z}\}$. Essa è quindi l'insieme dei numeri multipli di 3.
$[1]_3 = \{1 + 3h \ , \ h \in \mathbb{Z}\}$. Essa è quindi l'insieme dei numeri che, divisi per 3, hanno resto 1.
$[2]_3 = \{2 + 3h \ , \ h \in \mathbb{Z}\}$. Essa è quindi l'insieme dei numeri che, divisi per 3, hanno resto 2.
Si ha perciò $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$. △

Esercizio E.3.1 Determinare $\mathbb{Z}_4$.

Esercizio E.3.2 Determinare $\mathbb{Z}_5$.

Esercizio E.3.3 Determinare $\mathbb{Z}_1$.

Dato $n \in \mathbb{N}^*$,vogliamo ora determinare $\mathbb{Z}_n$. Gli esempi 3.9 e 3.10 e gli esercizi E.3.1 e E.3.2 dovrebbero averci dato l'idea. Si ha il seguente teorema.

Teorema 3.11 *Sia $n \in \mathbb{N}^*$. Allora:*

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-2]_n, [n-1]_n\}.$$

DIMOSTRAZIONE Per dimostrare ciò dobbiamo far vedere che ogni numero intero a appartiene ad una delle n classi scritte sopra e che tali classi sono tutte distinte. Dato un numero intero a, lo possiamo dividere per n in $\mathbb{Z}$ (vedere il teorema 3.3). Abbiamo cioè:
$a = qn + r$, $q \in \mathbb{Z},\ r \in \mathbb{Z}$, $0 \leq r < n$.
Da ciò deriva $[a]_n = [r]_n$. Abbiamo quindi visto che, se $a \geq 0$, esso appartiene ad una delle n classi scritte sopra.
Dobbiamo ora far vedere che le n classi di cui sopra sono tutte distinte. Basta far vedere che, dati $r \neq r'$ tali che $0 \leq r < n$ e $0 \leq r' < n$, allora $r \not\equiv r' \pmod{n}$. Supponiamo $r' > r$ (se $r' < r$ si invertono tra loro r e r'). Si ha quindi $0 < r' - r < n$. Supponiamo, per assurdo, che si abbia $r' \equiv r \pmod{n}$. Quindi $r' - r = qn$ con $q \in \mathbb{N}$. Abbiamo perciò $0 < r' - r = qn < n$; quindi $0 < qn < n$. Dividendo per n, si ottiene $0 < q < 1$. Il che è assurdo, essendo q un numero intero. ■

Nota 3.12 Per determinare la classe di congruenza modulo n cui appartiene un numero a positivo , dobbiamo quindi dividere a per n e considerare il resto r. Per questo motivo le classi di congruenza modulo n vengono anche chiamate **classi resto** modulo n. △

Teorema 3.13 *Si ha:*

$$a \equiv a' \pmod{n} \ , \ b \equiv b' \pmod{n} \Rightarrow a + b \equiv a' + b' \pmod{n}$$

*Diremo che l' operazione di addizione in $\mathbb{Z}$ è **compatibile** con la relazione di congruenza modulo n per ogni $n > 0$.*

DIMOSTRAZIONE Sia $a \equiv a' \pmod{n}$, $b \equiv b' \pmod{n}$. Quindi:
$a - a' = qn$, $b - b' = q'n$ con $q \in \mathbb{Z}$, $q' \in \mathbb{Z}$. Dobbiamo dimostrare che si ha $a+b \equiv a'+b' \pmod{n}$, cioè $(a+b)-(a'+b') = sn$ con $s \in \mathbb{Z}$. Sommando membro a membro si ha $(a + b) - (a' + b') = a - a' + b - b' = (q + q')n$. Ponendo ora $s = q + q'$, abbiamo $(a + b) - (a' + b') = sn$. □ ■

Il teorema precedente ci permette di dare la seguente:

Definizione 3.14 Introduciamo in $\mathbb{Z}_n$ la seguente operazione:

$$[a]_n + [b]_n = [a + b]_n$$

Chiamiamo questa operazione **addizione** in $\mathbb{Z}_n$. △

Nota 3.15 Osserviamo che il teorema precedente mostra che l'operazione di addizione appena definita è **ben posta**, non dipende cioè dalla scelta dei rappresentanti delle classi $[a]_n$ e $[b]_n$. △

Teorema 3.16 *L'operazione di addizione in $\mathbb{Z}_n$ verifica la proprietà associativa:*

$$[a]_n + ([b]_n + [c]_n) = ([a]_n + [b]_n) + [c]_n \quad \forall [a]_n \in \mathbb{Z}_p, \forall [b]_n \in \mathbb{Z}_p, \forall [c]_n \in \mathbb{Z}_n$$

la proprietà commutativa

$$[a]_n + [b]_n = [b]_n + [a]_n, \quad \forall [a]_n \in \mathbb{Z}_p, \forall [b]_n \in \mathbb{Z}_p$$

la proprietà di esistenza dell'elemento neutro e la proprietà di esistenza dell'opposto.

DIMOSTRAZIONE La proprietà associativa e la proprietà commutativa derivano dalle analoghe proprietà su $\mathbb{Z}$.
L'elemento neutro è $[0]_n$.
Dato $0 \leq a < n$, l'elemento opposto di $[a]_n$ è l'elemento $[n-a]_n$. Cioè:

$$-[a]_n = [n-a]_n$$

Esempio 3.17 Ecco la tabella dell'addizione di $\mathbb{Z}_2$:

	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

Notare che $[1]_2$ ha come opposto se stesso. △

Esempio 3.18 Ecco la tabella dell'addizione di $\mathbb{Z}_3$:

	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

Notare che $[1]_3$ e $[2]_3$ sono opposti tra loro. △

Esercizio E.3.4 Scrivere la tabella dell'addizione di $\mathbb{Z}_4$ e determinare l'opposto di ogni elemento.

Esercizio E.3.5 Scrivere la tabella dell'addizione di $\mathbb{Z}_5$ e determinare l'opposto di ogni elemento.

Fino a questo momento abbiamo considerato l'operazione di addizione in $\mathbb{Z}$ ed abbiamo considerato l'operazione indotta in $\mathbb{Z}_n$. D'ora in poi tentiamo di far lo stesso con l'operazione di moltiplicazione in $\mathbb{Z}$.

Teorema 3.19 *La relazione di congruenza modulo n è compatibile con l'operazione di moltiplicazione in $\mathbb{Z}$.*

DIMOSTRAZIONE Sia $a \equiv a' \pmod{n}$, $b \equiv b' \pmod{n}$. Quindi:
$a - a' = qn$, $b - b' = q'n$ con $q \in \mathbb{Z}$, $q' \in \mathbb{Z}$. Dobbiamo dimostrare che si ha $ab - a'b' = s'n$ con $s' \in \mathbb{Z}$. Si ha:
$ab - a'b' = ab - a'b + a'b - a'b' = (a-a')b + a'(b-b') = qnb + a'q'n = (qb + a'q')n$.
Da cui $s' = qb + a'q'$. Da cui la tesi. ■

Teorema 3.20 *Poiché l'operazione di moltiplicazione in $\mathbb{Z}$ è compatibile con la relazione di congruenza modulo n, è possibile definire su $\mathbb{Z}_n$ l'operazione di moltiplicazione nel seguente modo:*

$$[a]_n \cdot [b]_n = [a \cdot b]_n.$$

L'operazione di moltiplicazione verifica la proprietà associativa, la proprietà commutativa, e la proprietà di esistenza dell'elemento neutro.
E' valida infine la proprietà distributiva:

$$([a]_n + [b]_n)[c]_n = ([a]_n[c]_n) + [b]_n[c]_n \quad \forall [a]_n \in \mathbb{Z}_p, \forall [b]_n \in \mathbb{Z}_p, \forall [c]_n \in \mathbb{Z}_n$$

DIMOSTRAZIONE La proprietà associativa, la proprietà commutativa, la proprietà di esistenza dell'elemento neutro e la proprietà distributiva derivano dalle analoghe proprietà su $\mathbb{Z}$. La classe $[1]_n$ è l'elemento neutro rispetto alla moltiplicazione. ∎

Ci chiediamo ora se per ogni intero positivo n esista l'inverso di ogni elemento di $\mathbb{Z}_n$. Si verifica facilmente (esercizio) che ciò avviene per $n = 2$ e $n = 3$. Pertanto sia $\mathbb{Z}_2$ che $\mathbb{Z}_3$ con le operazioni di addizione e moltiplicazione sono campi. Si verifica poi che in $\mathbb{Z}_4$ la classe $[2]_4$ non è dotata di inverso. Pertanto $\mathbb{Z}_4$ non è un campo.

Dall'analisi della tabella della moltiplicazione di $\mathbb{Z}_5$:

	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

si osserva che ogni elemento non nullo è dotato di inverso. Pertanto $\mathbb{Z}_5$ è un campo.

Bene, abbiamo visto che $\mathbb{Z}_4$ non è un campo. Osserviamo anche che 4 non è un numero primo. Ciò è generalizzato dal seguente:

Teorema 3.21 *Sia n un numero intero positivo non primo. Allora $\mathbb{Z}_n$ con le usuali operazioni di addizione e moltiplicazione non è un campo.*

DIMOSTRAZIONE Sia $n = p \cdot q$ con $p \in \mathbb{N}, p \neq 1$ e $q \in \mathbb{N}, q \neq 1$.
Si ha poi $[p]_n \cdot [q]_n = [n]_n = [0]_n$. Ma $[p]_n \neq [0]_n$ e $[q]_n \neq [0]_n$. Sappiamo che in un campo il prodotto di due elementi non nulli è necessariamente non nullo. Ne segue che $\mathbb{Z}_n$ non è un campo. ∎

Nota 3.22 Osserviamo che gli elementi $[p]_n$ e $[q]_n$ di $\mathbb{Z}_n$ con $n = pq$ dati nel teorema precedente non sono dotati di inverso. Supponiamo infatti per assurdo che esista $[p]_n^{-1}$.
Moltiplicando ambo i membri dell'uguaglianza $[p]_n[q]_n = [0]_n$ per $[p]_n^{-1}$ si otterrebbe:

$$[p]_n^{-1}[p]_n[q]_n = [p]_n^{-1}[0]_n$$

da cui

$$[q]_n = [0]_n$$

il che è assurdo per ipotesi. △

Vogliamo dimostrare che, se n è primo, allora $\mathbb{Z}_n$ con le usuali operazioni di addizione e moltiplicazione è un campo. Per far ciò abbiamo bisogno di studiare alcune proprietà aritmetiche.

Definizione 3.23 Dati due numeri $p \in \mathbb{Z}$ e $a \in \mathbb{Z}$ si dice che p è **divisore** di a (o che p **divide** a) se esiste un numero $q \in \mathbb{Z}$ tale che $a = q \cdot p$. Per indicare che p divide a si usa il simbolo $p|a$. Spesso, quando $p|a$, si dice che a è un **multiplo** di p e che p è un **sottomultiplo** di a. △

Teorema 3.24 *Dati $d \in \mathbb{Z}$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ si ha:*
$d|a \ , \ d|b \Longrightarrow d|x \cdot a + y \cdot b \ \forall x \in \mathbb{Z} \ , \forall y \in \mathbb{Z}$.

Dimostrazione . Lasciata per esercizio. ■

Nota 3.25 In particolare si ha:
$d|a \Longrightarrow d|-a$ △

Nota 3.26 Dato comunque un numero $a \in \mathbb{Z}$, si ha che i numeri ± 1 e $\pm a$ sono divisori di a. △

Nota 3.27 Il numero 0 ha come divisori tutti i numeri $a \in \mathbb{Z}$. △

Definizione 3.28 Un numero $a \in \mathbb{Z}$ si dice **primo** se $a \neq \pm 1$ e gli unici divisori di a sono ± 1 e $\pm a$. △

Definizione 3.29 Dati $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}^*$ (quindi a e b sono numeri interi non nulli), un numero $d \in \mathbb{Z}$ si dice **massimo comun divisore** di a e b se esso verifica le seguenti condizioni:
1) $d > 0$
2) $d|a$ e $d|b$
3) se $d' \in \mathbb{Z}$ è tale che $d'|a$ e $d'|b$, allora $d'|d$.
Dimostreremo in 3.32 che, dati a e b, esiste ed è unico il loro massimo comun divisore. Il massimo comun divisore di a e b viene indicato con il simbolo $M.C.D.(a, b)$ oppure con il simbolo (a, b). Noi useremo di solito quest'ultimo.△

Teorema 3.30 *Dati $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}^*$, si ha:*

$$(a, b) = (|a|, |b|)$$

Dimostrazione . Si ha ovviamente:

$$d|a \Longleftrightarrow d|(-a)$$

Da ciò segue facilmente (esercizio) la tesi. ■

Nota 3.31 Possiamo perciò d'ora in poi limitarci a considerare il massimo comun divisore di numeri interi positivi. △

Teorema 3.32 *Dati $a \in \mathbb{N}$ e $b \in \mathbb{N}$, esiste ed è unico il loro massimo comun divisore.*

DIMOSTRAZIONE . Dimostriamo innanzitutto l'unicità. Siano d e d' massimi comun divisori di a e b. Si ha che d' divide sia a che b. Quindi, essendo d massimo comun divisore di a e b, si ha $d = p \cdot d'$ con $p \in \mathbb{N}$ poiché sia d che d' sono positivi. Analogamente si dimostra che si ha $d' = p' \cdot d$. Abbiamo allora: $d' = p' \cdot d = p' \cdot p \cdot d'$. Ne segue $1 = p' \cdot p$. Essendo p e p' interi positivi abbiamo $p = p' = 1$. Quindi $d = d'$.
Dimostriamo ora l'esistenza del massimo comun divisore. Determineremo il massimo comun divisore di $a \in \mathbb{N}$ e $b \in \mathbb{N}$ utilizzando un algoritmo, detto **algoritmo di Euclide**[1].
Per rendere più chiaro l'algoritmo, lo descriviamo innanzitutto scegliendo due numeri particolari $a = 2184$ e $b = 1980$. Vedremo in seguito che il procedimento seguito si applica ad una qualsiasi coppia di numeri naturali.
Cominciamo con il dividere il maggiore dei due numeri per l'altro:

$$\underline{2184} = \underline{1980} \cdot 1 + \underline{204}$$

Abbiamo sottolineato il dividendo, il divisore e il resto. Dividiamo il divisore per il resto:

$$\underline{1980} = \underline{204} \cdot 9 + \underline{144}$$

Continuiamo con lo stesso procedimento:

$$\underline{204} = \underline{144} \cdot 1 + \underline{60}$$

$$\underline{144} = \underline{60} \cdot 2 + \underline{24}$$

$$\underline{60} = \underline{24} \cdot 2 + \underline{12}$$

$$\underline{24} = \underline{12} \cdot 2 + 0$$

Quindi il numero 12 è l'ultimo resto non nullo. Dimostriamo che esso è il massimo comun divisore.
Innanzitutto 12 è un numero positivo. La prima condizione è quindi verificata. Dimostriamo ora che 12 divide i due numeri.
Dall'ultima uguaglianza segue che il numero 12, oltre a dividere ovviamente se stesso, divide anche 24. Dalla penultima uguaglianza, sfruttando il teorema 3.24, segue che 12 divide 60. Dalla terzultima uguaglianza segue che 12 divide 144. Analogamente 12 divide 204, quindi anche 1980 e quindi anche 2184. Abbiamo verificato che 12 è divisore comune di 2184 e 1980.
Dobbiamo ora verificare che esso è il massimo comun divisore. A tal scopo scriviamo i resti delle successive divisioni come combinazioni lineari del dividendo

[1] **Euclide**, (terzo-quarto secolo a.C.), matematico greco che descrisse l'algoritmo nei suoi "Elementi".

e del divisore:

$$\underline{204} = \underline{2184} + \underline{1980} \cdot (-1)$$
$$\underline{144} = \underline{1980} + \underline{204} \cdot (-9)$$
$$\underline{60} = \underline{204} + \underline{144} \cdot (-1)$$
$$\underline{24} = \underline{144} + \underline{60} \cdot (-2)$$
$$\underline{12} = \underline{60} + \underline{24} \cdot (-2)$$

Supponiamo ora che d' sia divisore comune di 2184 e 1980. Dalla prima delle uguaglianze precedenti segue che d' divide 204. Dalla seconda uguaglianza segue che d' divide 144; dalla terza segue che d' divide 60; dalla quarta segue che d' divide 24; dalla quinta segue che d' divide 12. Abbiamo dimostrato che 12 è il massimo comun divisore.

Possiamo utilizzare questo algoritmo per due numeri $a \in \mathbb{N}$ e $b \in \mathbb{N}$ qualsiasi. Se $a = b$, allora ovviamente $(a, b) = a = b$.
Sia $a > b$. Applichiamo il nostro algoritmo. Abbiamo:

$$\underline{a} = \underline{b} \cdot q_0 + \underline{r_0} \quad \text{con } 0 \leq r_0 < b$$
$$\underline{b} = \underline{r_0} \cdot q_1 + \underline{r_1} \quad \text{con } 0 \leq r_1 < r_0$$
$$\underline{r_0} = \underline{r_1} \cdot q_2 + \underline{r_2} \quad \text{con } 0 \leq r_2 < r_1$$
$$\dots$$
$$\underline{r_{n-2}} = \underline{r_{n-1}} \cdot q_n + \underline{r_n} \quad \text{con } 0 \leq r_n < r_{n-1}$$
$$\underline{r_{n-1}} = \underline{r_n} \cdot q_{n+1} + 0$$

Ad un certo punto dobbiamo necessariamente ottenere un resto uguale a 0 perchè la successione dei resti è una successione strettamente decrescente di numeri maggiori o uguali a 0. L'ultimo resto non nullo è il massimo comun divisore di a e b. Per dimostrare ciò basta seguire la falsariga della dimostrazione data nell'esempio numerico. Lasciamo per esercizio la dimostrazione dell'unicità. ■

Teorema 3.33 *Dati $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}^*$, sia d il massimo comun divisore di a e b. Allora esistono $x \in \mathbb{Z}$ e $y \in \mathbb{Z}$ che verificano la seguente* **identità di Bezout**[2]*:*

$$d = a \cdot x + b \cdot y$$

Dimostrazione . Consideriamo innanzitutto il caso in cui si abbia $a \in \mathbb{N}$ e $b \in \mathbb{N}$. Si applichi l'algoritmo di Euclide per determinare d. Esso è l'ultimo resto r_n non nullo. Dalla penultima identità si scrive r_n come combinazione lineare a coefficienti interi di r_{n-1} e di r_{n-2}. Poiché r_{n-1} è a sua volta combinazione lineare a coefficienti interi di r_{n-2} e di r_{n-3}, si scrive r_n come combinazione

[2]**Étienne Bèzout**,(1730-1783), matematico francese.

lineare di r_{n-2} e di r_{n-3}. Continuando in questo modo si scrive r_n come combinazione lineare di a e b.
Siano ora $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}^*$. Consideriamo i numeri $|a| \in \mathbb{N}$e $|b| \in \mathbb{N}$. Dal teorema 3.30 segue $d = (a, b) = (|a|, |b|)$. Per quel che abbiamo appena dimostrato, esistono $x' \in \mathbb{Z}$ e $y' \in \mathbb{Z}$ tali che $d = |a| \cdot x' + |b| \cdot y'$. Supponiamo che si abbia $a < 0$ e $b < 0$. Abbiamo allora $d = a \cdot (-x') + b \cdot (-y')$. Ponendo $x = -x'$ e $y = -y'$ abbiamo la tesi. Nel caso in cui $a > 0$ e $b < 0$ oppure $a < 0$ e $b > 0$ ci si comporta in modo analogo. ■

Nota 3.34 I numeri x e y dell'identità di Bezout non sono unici. Dimostriamo che ve ne sono infiniti.
Si ha ovviamente:
$0 = a \cdot b + b \cdot (-a)$. Quindi $\forall n \in \mathbb{Z}$ si ha $0 = a \cdot (b \cdot n) + b \cdot (-a \cdot n)$. Data allora l'identità di Bezout:

$$d = a \cdot x + b \cdot y$$

si ha $\forall n \in \mathbb{Z}$:

$$d = d + 0 = a \cdot x + b \cdot y + a \cdot (b \cdot n) + b \cdot (-a \cdot n) = a \cdot (x + b \cdot n) + b \cdot (y - a \cdot n)$$

Esempio 3.35 Vogliamo determinare l'identità di Bezout che lega i numeri 2184 e 1980 con il loro massimo comun divisore 12. Applicando l'algoritmo di Euclide avevamo trovato le seguenti identità:

$$\underline{204} = \underline{2184} + \underline{1980} \cdot (-1)$$

$$\underline{144} = \underline{1980} + \underline{204} \cdot (-9)$$

$$\underline{60} = \underline{204} + \underline{144} \cdot (-1)$$

$$\underline{24} = \underline{144} + \underline{60} \cdot (-2)$$

$$\underline{12} = \underline{60} + \underline{24} \cdot (-2)$$

Sostituiamo nell'ultima identità il numero 24 con la sua combinazione lineare di 144 e 60 (penultima identità) e così di seguito. Si ha:

$$\begin{aligned} \underline{12} = \underline{60} + \underline{24} \cdot (-2) = \underline{60} + [\underline{144} + \underline{60} \cdot (-2)] \cdot (-2) = \underline{144} \cdot (-2) + \underline{60} \cdot 5 = \\ = \underline{144} \cdot (-2) + [\underline{204} + \underline{144} \cdot (-1)] \cdot 5 = \underline{204} \cdot 5 + \underline{144} \cdot (-7) = \\ = \underline{204} \cdot 5 + [\underline{1980} + \underline{204} \cdot (-9)] \cdot (-7) = \underline{1980} \cdot (-7) + \underline{204} \cdot 68 = \\ = \underline{1980} \cdot (-7) + [\underline{2184} + \underline{1980} \cdot (-1)] \cdot 68 = \underline{2184} \cdot 68 + \underline{1980} \cdot (-75) \end{aligned}$$

Abbiamo quindi determinato l'identità di Bezout:

$$12 = 2184 \cdot 68 + 1980 \cdot (-75)$$

Esercizio E.3.6 Calcolare il massimo comun divisore dei numeri 73810 e 9318. Determinare quindi $x \in \mathbb{Z}$ e $y \in \mathbb{Z}$ tali che

$$(73810, 9318) = 73810 \cdot x + 9318 \cdot y$$

Esercizio E.3.7 Calcolare il massimo comun divisore dei numeri 73810 e -9318. Determinare quindi $x \in \mathbb{Z}$ e $y \in \mathbb{Z}$ tali che

$$(73810, -9318) = 73810 \cdot x + (-9318) \cdot y$$

Definizione 3.36 Due numeri $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}^*$ si dicono **primi tra loro** se hanno come divisore comune solamente i numeri ± 1.
Si ha quindi che a e b sono primi tra loro se e solo se $(a, b) = 1$. △

Esercizio E.3.8 Verificare se i numeri 37957 e 123957 sono primi tra loro.

3.3 Il campo $\mathbb{Z}_n$ per n primo

.

Teorema 3.37 *Sia $n \in \mathbb{N}$ un numero primo. Allora $\mathbb{Z}_n$ con le usuali operazioni di addizione e moltiplicazione è un campo.*

DIMOSTRAZIONE L'unica cosa che dobbiamo dimostrare che ogni classe $[a]_n \neq [0]_n$ è dotata di inverso in $\mathbb{Z}_n$.
Osserviamo che, poiché $[a]_n \neq [0]_n$, si ha che a non è multiplo di n. D'altronde n è un numero primo e quindi $(a, n) = 1$. Ma allora dall'identità di Bezout (vedere teorema 3.33) segue che esistono $x \in \mathbb{Z}$ e $y \in \mathbb{Z}$ tali che:

$$a \cdot x + n \cdot y = 1.$$

Da ciò segue $a \cdot x = 1 + (-y) \cdot n$. E quindi:

$$[a \cdot x]_n = [a]_n \cdot [x]_n = [1]_n$$

Pertanto:

$$[x]_n = [a]_n^{-1}$$

Abbiamo dimostrato il nostro teorema. ■

Nota 3.38 La dimostrazione del teorema precedente ci dà un algoritmo per determinare l'inverso di un elemento di $\mathbb{Z}_n$ se n è primo.
Cerchiamo, per esempio, l'inverso di $[10]_{23}$ in $\mathbb{Z}_{23}$. Sappiamo che il massimo comun divisore di 10 e 23 è 1. Utilizzando l'algoritmo di Euclide, possiamo determinare l'identità di Bezout che lega i numeri 1,10 e 23 (vedere teorema 3.33). Svolgendo i calcoli (esercizio) si ottiene l'identità di Bezout:

$$1 = 10 \cdot 7 + 23 \cdot (-3)$$

Quindi $[7]_{23} \cdot [10]_{23} = [1]_{23}$.
Pertanto abbiamo:

$$[10]_{23}^{-1} = [7]_{23}$$

3.4 Equazioni e sistemi lineari nel campo $\mathbb{Z}_n$

Abbiamo visto nel capitolo precedente che si possono estendere tutte le definizioni e i teoremi sui sistemi di equazioni lineari che abbiamo visto per il campo $\mathbb{R}$ al caso di un campo qualsiasi, quindi anche al caso del campo $\mathbb{Z}_n$, con n primo.

Esercizio E.3.9 Il numero 257 è primo. Quindi $[200]_{257}$ è dotato di inverso. Calcolarlo.

Esercizio E.3.10 Il numero 65537 è primo. Quindi $[200]_{65537}$ è dotato di inverso. Calcolarlo.

Esempio 3.39 Vogliamo determinare tutti i numeri interi x tali che:

$$2 \cdot x + 1 \equiv 4 \pmod 5$$

L'equazione di congruenze è equivalente alla seguente:

$$[2 \cdot x + 1]_5 = [4]_5$$

Utilizzando le operazioni di addizione e moltiplicazione nel campo $\mathbb{Z}_5$, si nota che l'equazione precedente coincide con la seguente equazione a coefficienti nel campo $\mathbb{Z}_5$:

$$[2]_5 \cdot [x]_5 + [1]_5 = [4]_5$$

Sottraendo ad ambo i membri $[1]_5$ otteniamo:

$$[2]_5 \cdot [x]_5 = [3]_5$$

Moltiplicando ambo i membri per $[2]_5^{-1} = [3]_5$, otteniamo:

$$[x]_5 = [3]_5 \cdot [3]_5 = [9]_5 = [4]_5$$

Tornando in $\mathbb{Z}$ otteniamo tutte le soluzioni dell'equazione originale:

$$x = 4 + 5h \mid h \in \mathbb{Z}$$

Esercizio E.3.11 Determinare tutti i numeri interi x tali che:

$$2 \cdot x + 4 \equiv 3 \pmod 5$$

Esercizio E.3.12 Determinare tutti i numeri interi x tali che:

$$20 \cdot x + 7 \equiv 3 \pmod{71}$$

Esercizio E.3.13 È vera la seguente affermazione:

$$a \cdot c \equiv b \cdot c \pmod n \iff a \equiv b \pmod n?$$

Esempio 3.40 Vogliamo determinare le soluzioni del sistema di congruenze:

$$\begin{cases} 4x+y & \equiv & 98 & (\text{mod } 5) \\ 2x+y & \equiv & 2351 & (\text{mod } 5) \end{cases}$$

Trasformiamo il sistema di congruenze in un sistema di equazioni nel campo $\mathbb{Z}_5$:

$$\begin{cases} [4]_5[x]_5+[y]_5 & = & [98]_5 & = & [3]_5 \\ [2]_5[x]_5+[y]_5 & = & [2351]_5 & = & [1]_5 \end{cases}$$

La matrice dei coefficienti ha determinante uguale a $[2]_5$. Esiste quindi una ed una sola soluzione. Calcoliamola utilizzando l'algoritmo di Cramer. Si ha:

$$[x]_5 = [2]_5^{-1} \cdot \det \begin{pmatrix} [3]_5 & [1]_5 \\ [1]_5 & [1]_5 \end{pmatrix} = [3]_5 \cdot ([3]_5 \cdot [1]_5 - [1]_5 \cdot [1]_5) = [3]_5 \cdot [2]_5 = [1]_5$$

$$[y]_5 = [2]_5^{-1} \det \begin{pmatrix} [4]_5 & [3]_5 \\ [2]_5 & [1]_5 \end{pmatrix} = [3]_5 \cdot ([4]_5 \cdot [1]_5 - [3]_5[2]_5) = [3]_5 \cdot [-2]_5 = [-6]_5 = [4]_5$$

Le soluzioni del nostro sistema di congruenze sono quindi:

$$\begin{cases} x = 1+5h \\ y = 4+5k \end{cases} \quad \forall h \in \mathbb{Z}\ , \forall k \in \mathbb{Z}$$

Esempio 3.41 Vogliamo determinare le soluzioni del sistema di congruenze:

$$\begin{cases} 13x-51y & \equiv & 501 & (\text{mod } 5) \\ 2001x+23y & \equiv & 77 & (\text{mod } 5) \end{cases}$$

Trasformiamo il sistema di congruenze in un sistema di equazioni nel campo $\mathbb{Z}_5$:

$$\begin{cases} [3]_5[x]_5+[4]_5[y]_5 & = [1]_5 \\ [1]_5[x]_5+[3]_5[y]_5 & = [2]_5 \end{cases}$$

La matrice dei coefficienti ha determinante uguale a $[0]_5$. È quindi necessario calcolare il rango della matrice A dei coefficienti e della matrice A' completa. Svolgendo i calcoli si nota che si ha:

$$\text{rk}(A) = \text{rk}(A') = 1$$

Il sistema ha quindi soluzioni.
Calcoliamo le soluzioni utilizzando l'algoritmo di Rouché-Capelli. Un minore invertibile della matrice A di ordine 1 è formato dalla prima riga e dalla prima colonna di A.
Consideriamo allora il sistema ridotto:

$$SR: \quad [3]_5[x]_5+[4]_5[y]_5 = [1]_5$$

Calcoliamo una soluzione particolare di SR. Poniamo $[y]_5 = [0]_5$ e otteniamo:

$$[3]_5[x]_5 = [1]_5$$

Da cui:

$$[x]_5 = [3]_5^{-1} = [2]_5$$

Una soluzione particolare è data quindi da:

$$([2]_5, [0]_5)$$

Consideriamo ora il sistema omogeneo associato:

$$SO: \quad [3]_5[x]_5 + [4]_5[y]_5 = [0]_5$$

Cerchiamo $Sol(SO)$. Poniamo $[y]_5 = [1]_5$ e otteniamo:

$$[3]_5[x]_5 + [4]_5[1]_5 = [0]_5$$

cioè:

$$[3]_5[x]_5 = [-4]_5 = [1]_5$$

da cui segue:

$$[x]_5 = [3]_5^{-1} = [2]_5$$

Si ha perciò:

$$([2]_5, [1]_5) \in Sol(SO)$$

Si ha allora:

$$Sol(SO) = \{([h]_5[2]_5, [h]_5[1]_5) \ , \ \forall [h]_5 \in \mathbb{Z}_5\}$$

Quindi le soluzioni di S sono date da:

$$Sol(S) = \{[2]_5 + [2]_5[h]_5, [0]_5 + [h]_5 \ , \forall [h]_5 \in \mathbb{Z}_5\}$$

Le soluzioni di S in $\mathbb{Z}_5$ dipendono da un parametro in $\mathbb{Z}_5$.
ATTENZIONE. Le soluzioni in $\mathbb{Z}_5$ non sono infinite. Si possono infatti assegnare a $[h]_5$ solo 5 valori.
Tornando al sistema in $\mathbb{Z}$, abbiamo:

$$Sol(S) = \{(2 + 2h + 5k, h + 5k') \ , \ \forall h = 0, 1, 2, 3, 4, \forall k \in \mathbb{Z}, \forall k' \in \mathbb{Z}\}$$

Esercizio E.3.14 Determinare tutte le eventuali soluzioni dei seguenti sistemi di congruenze:

$$\begin{cases} 3x + y \equiv 1 \pmod 3 \\ x - 2y \equiv 7 \pmod 3 \end{cases}$$

$$\begin{cases} 3x + y \equiv 1 \pmod 7 \\ x - 2y \equiv 7 \pmod 7 \end{cases}$$

$$\begin{cases} x + y + z \equiv 1 \pmod 5 \\ 6x + 13y + 26z \equiv -4 \pmod 5 \\ -4x + 121y - 3z \equiv 2011 \pmod 5 \end{cases}$$

Esercizio E.3.15 Determinare tutte le eventuali soluzioni dei seguenti sistemi di congruenze nei casi $n = 2, n = 3, n = 5, n = 7, n = 11$.

$$\begin{cases} x + y - z & \equiv & 2 & (\text{mod } n) \\ x & \equiv & 12 & (\text{mod } n) \\ x + y + 2z & \equiv & 13 & (\text{mod } n) \end{cases}$$

$$\begin{cases} x + y + z & \equiv & 1 & (\text{mod } n) \\ 2x - y - z & \equiv & 0 & (\text{mod } n) \\ 3x + y - 4z & \equiv & 2011 & (\text{mod } n) \end{cases}$$