

3.

I numeri interi

definizione dell'insieme \mathbb{Z}

operazioni in \mathbb{Z} e proprietà

congruenze modulo n

classi di resti modulo $n : \mathbb{Z}_n$

criteri di divisibilità

Se i numeri naturali nascono con l'uomo, con l'esigenza primordiale di contare, non si può dire lo stesso per i numeri negativi. Anche se essi vengono utilizzati già nel 1400 in campo mercantile per distinguere i debiti dai crediti, il loro ingresso nella ufficialità matematica occidentale è assai più tardo. Ancora nel XVII secolo Cartesio rifiutava di considerare "vere" le soluzioni negative di un'equazione, dato che i numeri negativi pretendono di rappresentare numeri *minori di nulla*; secondo A. Arnauld (1612-1694) i numeri negativi non esistono; dato che $-1:1=1:-1$, come è possibile che un minore stia a un maggiore come un maggiore a un minore? Ancora nel 1831 A. De Morgan (1806-1871) sostiene che quando un numero negativo compare come soluzione di un'equazione, allora si è in presenza di qualche assurdità.

L'insieme dei numeri interi si è dunque faticosamente imposto nella storia della matematica, e forse ancora oggi genera incomprensioni (si pensi per esempio al prodotto di due numeri negativi che dà un numero positivo); esso è tuttavia un insieme numerico importantissimo, perché in esso ogni elemento ammette opposto. Nell'insieme dei numeri interi ogni equazione del tipo $a+x=b$, (a differenza di quanto accade in \mathbb{N}) ammette sempre una ed una sola soluzione.

1. DAI NUMERI NATURALI AI NUMERI INTERI.

A partire dai numeri naturali possiamo definire tutti gli altri insiemi numerici, senza necessità di introdurre nuovi assiomi.

Vogliamo mostrare come sia possibile definire \mathbb{Z} , l'insieme dei *numeri interi relativi* (o semplicemente *numeri interi*)

$$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, +1, +2, +3, \dots \}$$

solo a partire da \mathbb{N} e dalle operazioni in esso introdotte.

Consideriamo il prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ di \mathbb{N} per se stesso.

In questo insieme introduciamo la relazione \sim , così definita:

$(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}: (a, b) \sim (c, d) \in \mathbb{N} \times \mathbb{N}$ se e solo se $a + d = b + c$.

Per esempio:

$$\begin{aligned} (5,2) &\sim (12,9), && \text{poiché } 5 + 9 = 2 + 12; \\ (12,9) &\sim (3,0), && \text{poiché } 12 + 0 = 9 + 3; \\ (1,5) &\sim (10,14), && \text{poiché } 1 + 14 = 5 + 10, \\ (3,2) &\not\sim (2,3), && \text{poiché } 3 + 3 \neq 2 + 2, \end{aligned}$$

e così via.

Da questi esempi si osserva che per ogni $k \in \mathbb{N}$ $(a,b) \sim (a+k, b+k)$.

La relazione introdotta è una relazione di equivalenza, cioè gode delle tre proprietà riflessiva, simmetrica, transitiva:

- *riflessiva*: $(a, b) \sim (a, b)$, poiché $a + b = b + a$ (per N2);
- *simmetrica*: se $(a, b) \sim (c, d)$ segue che $a + d = b + c$, e, sempre per N2 $d + a = c + b$, quindi $(c, d) \sim (a, b)$;
- *transitiva*: se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, allora $a + d = b + c$, e $c + f = d + e$; sommando membro a membro si ottiene: $a + d + c + f = b + c + d + e$, e per la legge di cancellazione della somma in \mathbb{N} (N9) $a + f = b + e$, cioè $(a, b) \sim (e, f)$.

Poiché la relazione " \sim " è una relazione di equivalenza in $\mathbb{N} \times \mathbb{N}$, possiamo considerare l'insieme quoziente $\mathbb{N} \times \mathbb{N} / \sim$, cioè l'insieme che ha per elementi le classi di equivalenza.

Determiniamo tali classi di equivalenza.

Fissato un elemento qualsiasi di $\mathbb{N} \times \mathbb{N}$, per esempio $(5, 2)$, quali sono le coppie ordinate (a, b) tali che $(a, b) \sim (5, 2)$?

Deve risultare

$$a + 2 = b + 5,$$

cioè

$$a - b = 5 - 2 = 3;$$

le coppie che appartengono alla stessa classe di equivalenza di $(5, 2)$ sono tutte quelle per le quali $a - b = 3$:

$$(3, 0), (4, 1), (6, 3), (7, 4), (8, 5), \dots, (n + 3, n), \dots$$

Quindi se $a > b$, ogni classe individua il numero naturale $a - b$; la classe di equivalenza rappresentata da tutte le coppie (a, a) è associata al numero naturale 0.

Se invece $a < b$, allora la classe a cui appartiene (a, b) non individua alcun numero naturale. Viene quindi spontaneo definire un nuovo insieme numerico, nel quale tutte le classi di equivalenza abbiano significato. Indichiamo la classe di equivalenza che contiene l'elemento (a, b) con il simbolo $[a, b]$.

DEFINIZIONE. Chiamiamo insieme dei *numeri interi*, e indichiamo con il simbolo \mathbb{Z} , l'insieme $\mathbb{N} \times \mathbb{N} / \sim$.

Chiamiamo

- *numeri interi positivi*: le classi $[a, b]$ con $a > b$;
- **0**: la classe $[a, a]$;
- *numeri interi negativi*: le classi $[a, b]$ con $a < b$.

numeri interi

Il sottoinsieme di \mathbb{Z} costituito dagli interi positivi e dallo **0** è in corrispondenza biunivoca con \mathbb{N} .

La classe

$$[0, 1] = \{(0, 1), (1, 2), (2, 3), \dots, (n, n + 1), \dots\}$$

individua il numero intero negativo -1 ; la classe

$$[0, 2] = \{(0, 2), (1, 3), (2, 4), \dots, (n, n + 2), \dots\}$$

individua il numero intero negativo -2 , e così via.

Se associamo ad ogni coppia ordinata (a, b) di numeri naturali il punto di coordinate (a, b) sul diagramma cartesiano di $\mathbb{N} \times \mathbb{N}$, i numeri interi (cioè le classi di equivalenza) si possono interpretare graficamente come le "semirette" di coefficiente angolare 1, come in figura 1.21.

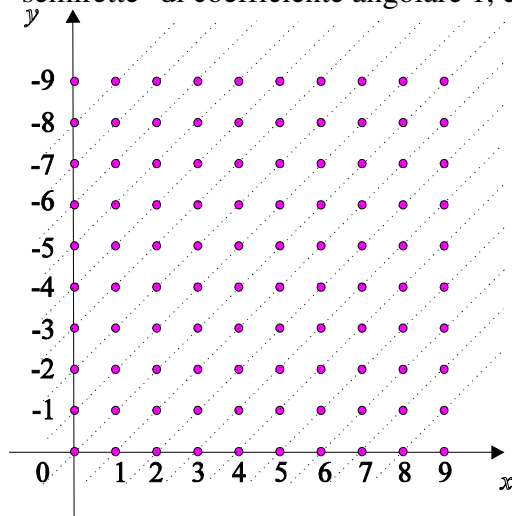


fig. 1.21

La bisettrice del quadrante è la semiretta di equazione $y = x$; essa corrisponde al numero 0 , e divide tutti i numeri positivi (le semirette che stanno "al di sotto" della bisettrice) da tutti i numeri negativi (le semirette "al di sopra" della bisettrice).

Possiamo sempre scegliere come rappresentante di un numero positivo la coppia $(a, 0)$, e come rappresentante di un numero negativo la coppia $(0, b)$.

Per indicare il numero intero $z \in \mathbb{Z}$ individuato dalla classe di equivalenza che contiene la coppia (a, b) usiamo la scrittura

$$z = [a, b],$$

mentre la coppia (a, b) è un *rappresentante* della classe di equivalenza. La distinzione non è pignoleria: i due numeri interi $[9, 4]$ e $[13, 8]$ coincidono, sono lo stesso numero, mentre le coppie $(9, 4)$, $(13, 8)$ sono due rappresentanti diversi di una stessa classe, cioè sono tra loro equivalenti; scriveremo dunque

$$[9, 4] = [13, 8] \quad \text{e invece} \quad (9, 4) \sim (13, 8).$$

La definizione di \mathbb{Z} che abbiamo dato sfrutta solo \mathbb{N} e le sue operazioni, come volevamo.

Definiamo ora le operazioni in \mathbb{Z} .

Dati i due numeri interi $[a, b]$, $[c, d]$, ne definiamo la "somma" nel seguente modo:

DEFINIZIONE . Se $[a, b], [c, d] \in \mathbb{Z}$, $[a, b] + [c, d] = [a + c, b + d]$.

addizione

Perché la definizione sia corretta, occorre dimostrare che il risultato non dipende dai rappresentanti scelti, e cioè se cambiano i rappresentanti, non cambia il risultato. Per esempio

$$[2, 5] + [3, 1] = [5, 6];$$

consideriamo diversi rappresentanti, per esempio $[4, 7]$, e $[8, 6]$; per definizione risulta

$$[4, 7] + [8, 6] = [12, 13];$$

il risultato è lo stesso, poiché

$$[12, 13] = [5, 6].$$

Dimostriamo questa proprietà in generale. Supponiamo $(a, b) \sim (a', b')$, e $(c, d) \sim (c', d')$; dobbiamo dimostrare che $(a + c, b + d) \sim (a' + c', b' + d')$;

Per ipotesi

$$a + b' = b + a' \quad \text{e} \quad c + d' = d + c';$$

sommando membro a membro

$$a + b' + c + d' = a' + b + c' + d$$

cioè

$$a + c + b' + d' = a' + c' + b + d,$$

che equivale a scrivere

$$(a + c, b + d) \sim (a' + c', b' + d').$$

cioè

$$[a, b] + [c, d] = [a', b'] + [c', d'].$$

Si dimostra facilmente che la somma in \mathbb{Z} è commutativa. Infatti

$$[a, b] + [c, d] = [a + c, b + d] = [c + a, d + b] = [c, d] + [a, b].$$

ESERCIZIO. Dimostrare che la somma in \mathbb{Z} è associativa.

DEFINIZIONE Dati $x, y \in \mathbb{Z}$, $x = [a, b]$, $y = [c, d]$, diciamo che x è maggiore di y , e scriviamo $x > y$, se e solo se

$$a + d > b + c.$$

ordinamento

Possiamo introdurre in \mathbb{Z} una relazione d'ordine totale nel seguente modo:

Per esempio $[6, 2] > [1, 3]$, poiché $6 + 3 > 2 + 1$. Non è difficile dimostrare che la definizione non dipende dai rappresentanti scelti.

Questa relazione è effettivamente una relazione d'ordine totale (in senso stretto). Infatti è

- *antisimmetrica*: se $[a, b] > [c, d]$ allora $a + d > b + c$, quindi non può valere $c + b > d + a$, cioè non vale $[c, d] > [a, b]$;
- *transitiva*: se $[a, b] > [c, d]$ e $[c, d] > [e, f]$ allora

$$a + d > b + c, \quad \text{e} \quad c + f > d + e,$$

da cui sommando

$$a + d + c + f > b + c + d + e,$$

e sottraendo $c + d$ da entrambi i membri si ottiene

$$a + f > b + e,$$

cioè $[a, b] > [e, f]$.

In \mathbb{Z} l'*elemento neutro* della somma è rappresentato dal numero $\mathbf{0} = [0, 0]$: per ogni $z \in \mathbb{Z}$ risulta $z + \mathbf{0} = z$.

elemento neutro

Caratteristica importante di \mathbb{Z} (a differenza di \mathbb{N}) è che ogni numero possiede l'*inverso rispetto alla somma* (detto anche l'*opposto*), cioè per ogni $z \in \mathbb{Z}$ esiste $z' \in \mathbb{Z}$ tale che

$$z + z' = [0, 0].$$

Infatti qualunque sia $z = [a, b]$, l'opposto di z è $z' = [b, a]$:

$$z + z' = [a, b] + [b, a] = [a + b, a + b] = [0, 0].$$

Indichiamo l'opposto di z con la scrittura $-z$.

elemento opposto

Ricordiamo che si definisce *valore assoluto* (o *modulo*) del numero intero z : il numero stesso se $z \geq \mathbf{0}$, il suo opposto $-z$ se $z < \mathbf{0}$. Il valore assoluto di z è indicato con il simbolo $|z|$.

valore assoluto $|z|$

Se $z = [a, b]$, e $a \geq b$, allora $|z| = [a, b]$, altrimenti $|z| = [b, a]$.

ESERCIZI

- A. Dimostrare che $\mathbf{0} = [0, 0]$ è maggiore di ogni numero negativo. Dimostrare che ogni numero positivo è maggiore di $\mathbf{0}$ e di ogni numero negativo.
- B. Dimostrare che $-(-z) = z$.
- C. Dimostrare che $|x| \cdot |y| = |xy|$.
- D. Dimostrare che se $|x - y| < 3$ allora $y - 3 < x < y + 3$.
- E. Dimostrare che in generale l'uguaglianza $|x-1| = |x|-1$ è falsa.

Ricordando che abbiamo definito positivo un numero intero $[a, b]$ se $a > b$, e negativo se $a < b$, è immediato dimostrare che la somma di due numeri positivi è un numero positivo, e la somma di due numeri negativi è un numero negativo.

Quando in un insieme esiste l'inverso di ogni elemento rispetto ad una operazione, allora è possibile definire l'operazione inversa come operazione diretta tra il primo elemento e l'inverso (rispetto a quella operazione) del secondo.

In \mathbb{Z} è possibile definire l'operazione inversa dell'addizione, la sottrazione, semplicemente nel modo seguente:

DEFINIZIONE Se $x, y \in \mathbb{Z}$ allora $x - y = x + (-y)$
--

<i>sottrazione</i>

cioè la differenza tra due numeri interi è uguale alla somma del primo e dell'opposto del secondo.

OSSERVAZIONE. Nella precedente definizione il segno "-" è scritto con due significati diversi: in " $x - y$ " è un simbolo di operazione, mentre in " $(-y)$ " significa "l'opposto di y "; in pratica, poiché $x + (-y) = x - y$, e $x - (-y) = x + y$, si tende a dimenticare tale distinzione.

Vogliamo ora definire il prodotto tra numeri interi. La definizione più naturale sembrerebbe la seguente:

Ipotesi di definizione. $[a, b] \cdot [c, d] = [ac, bd]$.

Secondo questa definizione risulterebbe per esempio

$$[5, 2] \cdot [1, 3] = [5, 6],$$

cioè $(+3) \cdot (-2) = (-1)$, risultato che non ha nulla a che fare con il prodotto di numeri interi che ben conosciamo.

Inoltre tale definizione non è comunque corretta, poiché il risultato dipende dal rappresentante scelto: essendo per esempio

$$[5, 2] = [8, 5] \quad \text{e} \quad [1, 3] = [4, 6],$$

dovrebbe risultare

$$[5, 2] \cdot [1, 3] = [8, 5] \cdot [4, 6],$$

mentre secondo la definizione data risulta

$$\begin{aligned} [5, 2] \cdot [1, 3] &= [5, 6] \\ [8, 5] \cdot [4, 6] &= [32, 30] \end{aligned}$$

e $[5, 6] \neq [32, 30]$.

Per avere una indicazione sulla definizione corretta osserviamo che il numero intero $[a, b]$ "corrisponde" alla differenza $(a - b)$. Il prodotto $[a, b] \cdot [c, d]$ "corrisponde" allora al prodotto

$$(a - b) \cdot (c - d) = (ac + bd) - (ad + bc).$$

Dati i due numeri interi $[a, b]$, $[c, d]$, ne definiamo dunque il prodotto nel seguente modo:

DEFINIZIONE Se $[a, b], [c, d] \in \mathbb{Z}$, $[a, b] \cdot [c, d] = [ac + bd, ad + bc]$.

moltiplicazione

Anche in questo caso non è difficile dimostrare che il risultato non dipende dai rappresentanti scelti per x e y .

ESEMPIO 1. Calcolare il prodotto tra $x = [2, 5]$ e $y = [3, 1]$.

Per definizione risulta

$$[2, 5] \cdot [3, 1] = [6 + 5, 2 + 15] = [11, 17] = [0, 6].$$

Come si vede i conti "tornano", cioè se interpretiamo $[2, 5]$ come il numero negativo -3 , e $[3, 1]$ come $+2$, il loro prodotto è -6 . Proviamo a cambiare i rappresentanti; risulta

$$[4, 7] \cdot [6, 4] = [24 + 28, 16 + 42] = [52, 58] = [0, 6].$$

TEOREMA. Il prodotto in \mathbb{Z} è commutativo.

Dimostrazione. Siano $x = [a, b]$ e $y = [c, d]$. Allora

$$\begin{aligned}xy &= [a, b] \cdot [c, d] = [ac + bd, ad + bc] = [ca + db, cb + da] = \\ &= [c, d] \cdot [a, b] = yx.\end{aligned}$$

TEOREMA. In \mathbb{Z} vale la legge di cancellazione del prodotto : se

$$xy = xz \text{ e } x \neq 0, \text{ allora } y = z.$$

Dimostrazione. Siano $y = [c, d]$ e $z = [e, f]$. Se $x \neq 0$ allora x è positivo oppure negativo; distinguiamo i due casi. Se x è positivo lo possiamo rappresentare mediante una opportuna coppia $[a, 0]$, con $a \neq 0$. Poiché

$$xy = [a, 0] \cdot [c, d] = [ac, ad]$$

e

$$xz = [a, 0] \cdot [e, f] = [ae, af];$$

allora se $xy = xz$ risulta $[ac, ad] = [ae, af]$, cioè

$$ac + af = ad + ae,$$

$$a(c + f) = a(d + e),$$

e per la legge di cancellazione in \mathbb{N}

$$c + f = d + e,$$

cioè $[c, d] = [e, f]$: $y = z$. Possiamo svolgere un ragionamento del tutto analogo se x è negativo.

Si può dimostrare facilmente che l'*elemento neutro* del prodotto è il numero intero $[1, 0]$. Infatti per ogni $[a, b] \in \mathbb{Z}$ risulta

$$[a, b][1, 0] = [a + 0, 0 + b] = [a, b].$$

ESERCIZI

- A** Dimostrare che il prodotto in \mathbb{Z} è associativo.
- B** Dimostrare che in \mathbb{Z} vale la proprietà distributiva del prodotto rispetto alla somma.
- C** Dimostrare che $z \cdot [0, 1] = -z$.
- D** Dimostrare che per ogni $z \in \mathbb{Z}$ risulta $z \cdot [0, 0] = [0, 0]$.

Come in \mathbb{N} , anche in \mathbb{Z} non esiste in generale l'elemento inverso rispetto al prodotto.

Possiamo ora facilmente dimostrare una della proprietà più curiose dei numeri interi, e cioè che il prodotto di due numeri negativi è un numero positivo.

TEOREMA. Il prodotto di due numeri negativi è un numero positivo.

Dimostrazione. Infatti siano x e y due numeri interi negativi; per un numero negativo (cioè un numero $[h, k]$ con $h < k$) possiamo sempre scegliere come rappresentante la coppia il cui primo elemento sia 0. Quindi possiamo porre $x = [0, a]$ e $y = [0, b]$. Segue

$$x \cdot y = [0, a] \cdot [0, b] = [ab, 0];$$

il risultato è un numero il cui primo elemento è maggiore del secondo, cioè è un numero intero positivo.

In particolare $[0, 1] \cdot [0, 1] = [1, 0]$, cioè $(-1) \cdot (-1) = +1$.

ESERCIZIO. Dimostrare che il prodotto di un numero positivo e di un numero negativo è negativo, e che il prodotto di due numeri positivi è positivo.

OSSERVAZIONE. Quelle che vengono usualmente chiamate "regole dei segni" sono in realtà delle proprietà dimostrabili dei numeri interi.

Abbiamo così visto come sia possibile costruire \mathbb{Z} mediante i numeri naturali, in modo rigoroso e senza far ricorso a nuovi assiomi. Raggiunto questo scopo, possiamo tranquillamente tornare a scrivere i numeri interi nel solito modo.

ESERCIZIO Eseguire le seguenti operazioni facendo ricorso alle definizioni studiate, dopo aver ricondotto ogni numero alla classe di equivalenza di cui può essere visto come rappresentante, seguendo lo schema indicato dalla prima.

- $(-3) + (5) = [2, 5] + [6, 1] = [8, 6] = +2$
- $(-45) \cdot (+2) + (-4) =$
- $(-2) \cdot (-10) \cdot (-1) =$
- $(3) + (7) \cdot (-3) + (8) \cdot (-7) =$

Esplicitare le proprietà a cui si è dovuto far ricorso ad ogni passaggio.

2. LE CONGRUENZE

È nota la suddivisione dei numeri interi in pari e dispari; la suddivisione di tutti i numeri interi in classi si può generalizzare, per esempio suddividendo i numeri interi in 3 classi: i numeri multipli di 3, cioè della forma $3k$, i numeri della forma $3k + 1$, e infine i numeri della forma $3k + 2$.

$$\begin{aligned} & \dots, -9, -6, -3, 0, 3, 6, 9, \dots, 3k, \dots \\ & \dots, -8, -5, -2, 1, 4, 7, 10, \dots, 3k + 1, \dots \\ & \dots, -7, -4, -1, 2, 5, 8, 11, \dots, 3k + 2, \dots \end{aligned}$$

A questo scopo, vogliamo introdurre in \mathbb{Z} una opportuna relazione di equivalenza.

Siano $x, y \in \mathbb{Z}$, $y \neq 0$; esistono due numeri $q, r \in \mathbb{Z}$, con $0 \leq r < |y|$, tali che

$$x = qy + r.$$

Con queste richieste q e r risultano univocamente determinati per ogni coppia $x, y \in \mathbb{Z}$: q risulta essere il massimo intero tale che

$$qy < x,$$

e quindi

$$r = x - qy.$$

Esistenza e unicità di
quoziente e resto in \mathbb{Z}

Vediamo qualche esempio nella seguente tabella:

x	y	q	r
-8	3	-3	1
-8	-3	3	1
8	-3	-2	2
8	3	2	2

In questo modo è possibile estendere all'insieme dei numeri interi \mathbb{Z} la definizione delle operazioni *div* e *mod* che abbiamo già dato in \mathbb{N} , ponendo

$$q = x \operatorname{div} y \quad \text{e} \quad r = x \operatorname{mod} y.$$

Fissato n , gli unici risultati possibili dell'operazione $m \operatorname{mod} n$, con $m, n \in \mathbb{Z}$, e $n > 1$, sono i numeri

$$0, 1, 2, \dots, n - 1.$$

Introduciamo in \mathbb{Z} la relazione di *congruenza*:

DEFINIZIONE. Diremo che due numeri $a, b \in \mathbb{Z}$ sono *congrui modulo n* , e scriveremo

$$a \equiv b \pmod{n},$$

se e solo se

$$a \operatorname{mod} n = b \operatorname{mod} n.$$

Cioè: a e b sono congrui modulo n se, divisi per n , danno lo stesso resto; per esempio

$$19 \equiv 4 \pmod{5}$$

$$27 \equiv 12 \pmod{5}$$

$$-1 \equiv 4 \pmod{5}$$

$$-27 \equiv 3 \pmod{10}$$

$$100 \equiv 1 \pmod{3}$$

$$64 \equiv 0 \pmod{8}$$

mentre invece

$$7 \not\equiv 12 \pmod{4}$$

$$-1 \not\equiv 1 \pmod{5}$$

OSSERVAZIONE. Il termine "congruenza" è utilizzato anche in geometria: due segmenti sono congruenti se hanno la stessa lunghezza. Nel caso che stiamo esaminando le lunghezze non c'entrano: l'analogia consiste nel fatto che in entrambi i casi si tratta (come mostreremo tra poco per la congruenza in \mathbb{Z}) di una relazione di equivalenza. Forse più semplicemente dovremmo utilizzare, in tutti questi casi, proprio il termine "equivalenza", specificando ogni volta quale sia la relazione che definisce quella particolare equivalenza. Si pensi ai diversi ambiti in cui si usa dire, di due oggetti, che "sono equivalenti": due figure piane che abbiano la stessa area, due solidi che abbiano lo stesso volume, due frazioni che individuano lo stesso numero razionale, e così via.

Si può dare una definizione di congruenza tra numeri interi del tutto equivalente alla precedente, come mostra il seguente:

TEOREMA. $a \equiv b \pmod{n}$ se e solo se $a - b = kn$ per un opportuno $k \in \mathbb{Z}$ (cioè se $a - b$ è un multiplo di n).

Dimostrazione.

I) Se $a \operatorname{mod} n = b \operatorname{mod} n$, allora

$$\begin{aligned} a &= q_1 n + r, \\ b &= q_2 n + r, \end{aligned}$$

e sottraendo membro a membro

$$a - b = q_1 n + r - q_2 n - r = (q_1 - q_2)n,$$

cioè $a - b$ è multiplo di n .

II) Sia $a - b = kn$. Esistono, e sono univocamente determinati, q_1 e r_1 , q_2 e r_2 , tali che

$$\begin{aligned} a &= q_1 n + r_1 \\ b &= q_2 n + r_2 \end{aligned}$$

risulta quindi

$$\begin{aligned} a - b &= (q_1 - q_2)n + r_1 - r_2 = kn, \\ r_1 - r_2 &= (k - q_1 + q_2)n; \end{aligned}$$

cioè $r_1 - r_2$ è multiplo di n ; ma poiché

$$0 \leq r_1 < n \quad \text{e} \quad 0 \leq r_2 < n,$$

allora $-n < r_1 - r_2 < n$, e quindi necessariamente $k - q_1 + q_2 = 0$, cioè

$$r_1 = r_2.$$

ESEMPIO 2. Risulta $26 \equiv 14 \pmod{3}$. Infatti, secondo la definizione

$$26 \pmod{3} = 14 \pmod{3} = 2;$$

d'altra parte, in accordo col teorema dimostrato:

$$26 - 14 = 12 = 4 \cdot 3.$$

Lasciamo come esercizio la dimostrazione del seguente

TEOREMA. La relazione di congruenza modulo n , definita in \mathbb{Z} , è una relazione di equivalenza.

3. LE CLASSI DI RESTO MODULO n : \mathbb{Z}_n .

Poichè la relazione di congruenza modulo n è una relazione di equivalenza, è possibile suddividere l'insieme \mathbb{Z} in classi di equivalenza (gli elementi dell'insieme quoziente \mathbb{Z}/\equiv), ciascuna delle quali contiene tutti i numeri interi congrui tra loro modulo n . Poiché i possibili resti nella divisione per n sono i numeri

$$0, 1, 2, \dots, n - 1,$$

allora le classi di equivalenza, chiamate *classi di resto modulo n* , sono esattamente n ; di ciascuna classe possiamo scegliere come rappresentante il numero compreso tra 0 e $n - 1$ che vi appartiene, di modo che ogni numero intero appartenga ad una e una sola delle n classi

$$[0], [1], [2], \dots, [n - 1],$$

Per esempio, se $n = 5$, tutti gli interi si possono suddividere in 5 classi:

$$\begin{aligned} &\{ \dots, -15, -10, -5, 0, 5, 10, 15, \dots, 5k, \dots \} \\ &\{ \dots, -14, -9, -4, 1, 6, 11, 16, \dots, 5k + 1, \dots \} \\ &\{ \dots, -13, -8, -3, 2, 7, 12, 17, \dots, 5k + 2, \dots \} \\ &\{ \dots, -12, -7, -2, 3, 8, 13, 18, \dots, 5k + 3, \dots \} \\ &\{ \dots, -11, -6, -1, 4, 9, 14, 19, \dots, 5k + 4, \dots \} \end{aligned}$$

Ogni numero intero appartiene a una e una sola classe: l'insieme delle classi costituisce una partizione di \mathbb{Z} .

Indicheremo con il simbolo \mathbb{Z}_n l'insieme delle classi di resto modulo n , quindi l'insieme quoziente \mathbb{Z}/\equiv .

ESERCIZIO

Scrivere le partizioni di \mathbb{Z} a cui si perviene operando come in precedenza per $n = 2$ ed $n = 7$.

Le congruenze sono spesso presenti nella vita comune, quando l'insieme numerico che si utilizza ha una struttura *ciclica*: per esempio le ore dell'orologio sono indicate modulo 12 (oppure modulo 24), i giorni della settimana sono indicati modulo 7, le ampiezze degli angoli modulo 360, e così via.

Fissiamo un certo numero intero $n > 1$, rispetto al quale consideriamo la relazione di congruenza. Vale il seguente fondamentale

TEOREMA. Se $a \equiv b$ e $c \equiv d$, allora $a + c \equiv b + d$, e $ac \equiv bd$.

Le congruenze conservano la somma e il prodotto

Dimostrazione. Per ipotesi $a - b = hn$ e $c - d = kn$, quindi sommando membro a membro

$$a + c - (b + d) = (h + k)n,$$

cioè $a + c \equiv b + d$. Inoltre se $a - b = hn$ e $c - d = kn$, allora $a = b + hn$ e $c = d + kn$, e moltiplicando membro a membro

$$ac = bd + hnd + knb + hkn^2 = bd + (hd + kb + hkn)n,$$

da cui

$$ac - bd = (hd + kb + hkn)n,$$

cioè $ac \equiv bd$.

OSSERVAZIONE. Conseguenze immediate di questo teorema sono le seguenti:

$$a + b \equiv (a \bmod n) + (b \bmod n) \pmod{n}$$

$$a \cdot b \equiv (a \bmod n) \cdot (b \bmod n) \pmod{n}$$

Per esempio, modulo 7:

$$26 + 51 \equiv (26 \bmod 7) + (53 \bmod 7) \equiv 5 + 4 \equiv 2,$$

e

$$26 \cdot 51 \equiv (26 \bmod 7) \cdot (53 \bmod 7) \equiv 5 \cdot 4 \equiv 6.$$

Il teorema appena dimostrato ci permette di definire le operazioni di addizione e moltiplicazione nell'insieme \mathbb{Z}_n :

ADDIZIONE. $[a] + [b] = [a + b]$.

MOLTIPLICAZIONE. $[a] \cdot [b] = [ab]$.

Per esempio, se $n = 10$, allora in \mathbb{Z}_{10} risulta

$$[7] + [6] = [3], \quad [7] \cdot [6] = [2].$$

Il fatto che tali definizioni siano corrette, cioè che il risultato non dipenda dal rappresentante, è una diretta conseguenza del teorema sopra dimostrato.

Ecco finalmente smentito il luogo comune secondo cui "2 + 2 fa sempre 4": infatti nell'insieme delle classi di resto modulo 3

$$[2] + [2] = [1].$$

ESERCIZI

A. Calcolare $[3] + [4]$ e $[3][4]$ in \mathbb{Z}_6 ed in \mathbb{Z}_5 .

B. Calcolare:

- $[2] + [2] + [1]$ e $[2][2]$ in \mathbb{Z}_3 ;
- $[2] + [3] + [1] + [2]$ e $[2][3]$ in \mathbb{Z}_4 ;
- $[2] + [7] + [1] + [4]$ e $[4][5]$ in \mathbb{Z}_8 ;
- $[6] + [5]$ e $[2][3][2][5]$ in \mathbb{Z}_7 ;
- $[3] + [1]$ e $[3][2][3]$ in \mathbb{Z}_4 e in \mathbb{Z}_{10} ;
- $[4] + [6] + [5] + [2] + [3]$ e $[5][6]$ in \mathbb{Z}_7 e in \mathbb{Z}_{12} .

A quali proprietà della somma e del prodotto nelle classi di resti si è dovuto far riferimento?

Dimostrare queste proprietà, esplicitando a quali proprietà di \mathbb{N} si deve far riferimento.

Qual è il modo più rapido di eseguire queste operazioni?

Le operazioni di addizione e moltiplicazione in \mathbb{Z}_n possono essere ben visualizzate per mezzo delle tavole pitagoriche; per esempio in \mathbb{Z}_5 le tavole pitagoriche dell'addizione e della moltiplicazione sono le seguenti (per semplicità di scrittura indichiamo solo i rappresentanti):

+	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

L'insieme \mathbb{Z}_n costituisce un interessante esempio di insieme numerico finito e tuttavia "autosufficiente" rispetto alle operazioni di addizione e moltiplicazione, il cui risultato appartiene sempre a \mathbb{Z}_n .

*proprietà delle operazioni
in \mathbb{Z}_n*

Se analizziamo più da vicino questa struttura, scopriamo interessanti analogie e ancor più interessanti differenze rispetto agli insiemi numerici sin qui analizzati, cioè \mathbb{N} e \mathbb{Z} .

Supponiamo di fissare un qualsiasi $n > 1$.

In \mathbb{Z}_n esiste l'elemento neutro della somma: è il "numero" $[0]$.

Per ogni $z \in \mathbb{Z}_n$ esiste l'opposto (l'inverso rispetto alla somma), cioè l'elemento $z' \in \mathbb{Z}_n$ tale che $z + z' = [0]$. Infatti l'opposto di $[a]$ è $[n - a]$. Per esempio in \mathbb{Z}_5 l'opposto di $[4]$ è $[1]$, e l'opposto di $[3]$ è $[2]$, l'opposto di $[0]$ è $[0]$. Dunque in \mathbb{Z}_n è sempre possibile eseguire la sottrazione tra due elementi.

In \mathbb{Z}_n esiste l'elemento neutro del prodotto: $[1]$.

Queste sono tutte proprietà di cui gode anche \mathbb{Z} .

In \mathbb{Z}_n (a differenza di quanto accade in \mathbb{N} e in \mathbb{Z}) non vale in generale la *legge di annullamento del prodotto*: se $ab = 0$ allora $a = 0$ oppure $b = 0$.

Tale legge, del tutto evidente in \mathbb{N} e in \mathbb{Z} , dice in sostanza che due numeri entrambi diversi da 0 (cioè diversi dall'elemento neutro della somma) non possono dare come prodotto 0. Questo in generale non è vero in \mathbb{Z}_n .

Infatti se consideriamo l'insieme delle classi di resto rispetto a un numero n non primo, per esempio $n = 6$, risulta

$$[3] \cdot [2] = [0];$$

si dice in questo caso che [3] e [2] sono *divisori dello zero*. In \mathbb{N} e in \mathbb{Z} non ci sono divisori dello 0, in \mathbb{Z}_n , se $n = ab$, a e b sono divisori dello 0.

In altri termini: in generale non vale, in \mathbb{Z}_n , la legge di cancellazione per il prodotto: se

$$ac \equiv bc \pmod{n}$$

non è detto che in generale risulti

$$a \equiv b \pmod{n}.$$

Per esempio:

$$5 \cdot 2 \equiv 8 \cdot 2 \pmod{6}$$

ma è falso dedurne

$$5 \equiv 8 \pmod{6}.$$

Vedremo più avanti che la legge di cancellazione per il prodotto vale se $\text{MCD}(c, n) = 1$.

Se esaminiamo la tavola pitagorica di \mathbb{Z}_5 rispetto al prodotto, osserviamo una importante novità rispetto a \mathbb{Z} : ogni elemento diverso da [0] possiede l'inverso (rispetto al prodotto). Infatti

$$[2] \cdot [3] = [1] \quad [4] \cdot [4] = [1] \quad [1] \cdot [1] = [1].$$

Come dimostreremo più avanti, questa è una proprietà generale di tutti gli insiemi \mathbb{Z}_p , con p numero primo. In \mathbb{Z}_p è possibile dunque definire l'operazione inversa del prodotto, cioè la *divisione* per un numero diverso da [0]. Per esempio, in \mathbb{Z}_5 risulta

$$[4] / [3] = [4] \cdot [2] = [3].$$

ESERCIZIO Trovare gli inversi di tutti gli elementi di \mathbb{Z}_7 diversi da [0].

Se n è primo, allora è possibile operare in \mathbb{Z}_n con le quattro operazioni elementari (non è definita solo la divisione per [0]).

Vediamo ora qualche applicazione delle congruenze.

Il Teorema di Wilson

La relazione di congruenza tra numeri interi ci permette di enunciare un risultato di notevole importanza, la cui dimostrazione verrà fornita in un capitolo successivo. Esso fornisce una condizione necessaria e sufficiente affinché un numero intero p sia primo.

TEOREMA (di Wilson). Condizione necessaria e sufficiente affinché p sia primo è che

$$(p - 1)! \equiv p - 1 \pmod{p}.$$

ESEMPIO 3. Se $p = 7$:

$$6! = (6 \cdot 5) \cdot (4 \cdot 3 \cdot 2) \equiv 2 \cdot 3 \equiv 6 \pmod{7}.$$

Se $p = 11$:

$$10! = (10 \cdot 9) \cdot (8 \cdot 7) \cdot (6 \cdot 5) \cdot (4 \cdot 3 \cdot 2) \equiv 2 \cdot 1 \cdot 8 \cdot 2 \equiv 10 \pmod{11}$$

OSSERVAZIONE. Per calcolare $6! \pmod{7}$ e $10! \pmod{7}$ non è necessario calcolare $6!$ e $10!$, ma si può usare la proprietà associativa del prodotto e sostituire ad ogni fattore il suo resto modulo n .

Il teorema di Wilson permette di determinare se p è primo con un nuovo e semplicissimo algoritmo:

Algoritmo per riconoscere se p è primo con il Teorema di Wilson

leggi(p)

$a:=1$

per $i:=2$ fino a $p-1$ fai

$a:=(a \cdot i) \bmod p$

se $a = p-1$ allora scrivi ('è primo')
altrimenti scrivi ('è composto').

4. I CRITERI DI DIVISIBILITÀ

È facile riconoscere se un numero è divisibile per 3: basta verificare se la somma delle cifre è divisibile per 3. Qual è la giustificazione teorica di questo metodo? Inoltre: esiste un criterio di divisibilità anche per 7, per 11, o per 39?

Per definizione un numero $a \in \mathbb{Z}$ è un divisore di n se esiste $k \in \mathbb{Z}$ tale che $a = kn$. Da quanto abbiamo visto sinora, possiamo dare una definizione del tutto equivalente di divisibilità, sfruttando le congruenze.

DEFINIZIONE. $a \in \mathbb{Z}$ è divisibile per $n \neq 0$ (o equivalentemente n è un divisore di a) se e solo se $a \equiv 0 \pmod{n}$.

È del tutto evidente l'equivalenza delle due definizioni.

OSSERVAZIONE. La relazione di divisibilità è una relazione antisimmetrica in \mathbb{N} : infatti se a divide b , e b divide a , allora $a = b$. La relazione di divisibilità non è antisimmetrica in \mathbb{Z} : infatti, ad esempio, -2 divide 2 , 2 divide -2 , tuttavia $-2 \neq 2$.

Sia dato $x \in \mathbb{Z}$, vogliamo sapere se x è divisibile per d ; supponiamo per semplicità che sia $x > 0$ (è evidente che x è divisibile per d se e solo se $-x$ lo è).

Sappiamo che x ammette la rappresentazione polinomiale in base 10:

$$x = a_n 10^n + \dots + a_1 10 + a_0,$$

dove il generico coefficiente a_i è uguale a una delle cifre $0, 1, 2, \dots, 9$.

Consideriamo le congruenze modulo 3.

Da quanto abbiamo sinora visto, risulta $10 \equiv 1 \pmod{3}$; elevando al quadrato entrambi i membri della congruenza:

$$10^2 \equiv 1 \pmod{3};$$

e in generale, per ogni h ,

$$10^h \equiv 1 \pmod{3}.$$

Moltiplicando ambo i membri per a risulta che, qualunque sia h :

$$a \cdot 10^h \equiv a \pmod{3}.$$

Quindi

$$x = a_n 10^n + \dots + a_1 10 + a_0 \equiv a_n + \dots + a_1 + a_0 \equiv \sum_{i=0}^n a_i.$$

divisibilità per 3

Questo significa che x è divisibile per 3, cioè $x \equiv 0 \pmod{3}$, se e solo se è divisibile per 3 la somma delle sue cifre.

Per esempio, $x = 1789$:

$$1789 = 1000 + 700 + 80 + 9 \equiv 1 + 7 + 8 + 9 \equiv 1 + 1 + 2 + 0 \equiv 1 \pmod{3}.$$

1789 non è divisibile per 3, poiché $1789 \not\equiv 0$, bensì $1789 \equiv 1$: è un numero della forma $3k + 1$.

Il criterio di divisibilità per 9 è analogo, poiché vale la congruenza

$$10^h \equiv 1 \pmod{9}$$

divisibilità per 9

per ogni esponente h :

un numero è divisibile per 9 se e solo se è divisibile per 9 la somma delle sue cifre.

Per esempio 1782 è divisibile per 9: $1 + 7 + 8 + 2 = 18$.

I criteri di divisibilità per 2 e per 5 sono immediati; qualunque sia x , esso si può sempre esprimere nel seguente modo:

$$x = 10n + a_0,$$

dove a_0 è la cifra delle unità; e poiché $10 \equiv 0$ sia modulo 2 che modulo 5, allora $10n \equiv 0$, perciò

divisibilità per 2 o 5

$$x \equiv a_0 \pmod{2} \text{ e } x \equiv a_0 \pmod{5}$$

cioè x è divisibile per 2 o per 5 se lo è la sua cifra delle unità.

In modo analogo possiamo dimostrare i criteri di divisibilità per 4 e per 25 (cioè per 2^2 e per 5^2).

divisibilità per 4 o 25

Scriviamo x nel seguente modo:

$$x = 100a_2 + 10a_1 + a_0.$$

Poiché $100 \equiv 0 \pmod{4}$, e $100 \equiv 0 \pmod{25}$, allora

$$x = 100a_2 + 10a_1 + a_0 \equiv 10a_1 + a_0;$$

cioè x è divisibile per 4 (o per 25) se e solo se è divisibile per 4 (per 25) il numero costituito dalle sue ultime due cifre.

Per esempio, 17834 non è divisibile per 4 perché non lo è 34, mentre 12345675 è divisibile per 25, poiché lo è 75.

Generalizzando, possiamo determinare i criteri di divisibilità per 2^n , o per 5^n ; infatti $10^n \equiv 0$ sia modulo 2^n che modulo 5^n , quindi un numero è divisibile per 2^n (o per 5^n) se lo è il numero costituito dalle sue ultime n cifre.

divisibilità per 2^n o 5^n

Per esempio 876128 è divisibile per 8, poiché 128 lo è.

Valutiamo ora la divisibilità per 11.

divisibilità per 11

Risulta

$$10^0 \equiv 1 \pmod{11}$$

$$10^1 \equiv -1 \pmod{11};$$

calcolando le successive potenze di entrambi i membri:

$$10^2 \equiv (-1)^2 \equiv 1 \pmod{11}$$

$$10^3 \equiv (-1)^3 \equiv -1 \pmod{11}$$

$$10^4 \equiv (-1)^4 \equiv 1 \pmod{11}$$

...

quindi le successive potenze di 10 sono congrue a 1 se l'esponente è pari, e congrue a -1 se l'esponente è dispari. Per un numero x qualsiasi risulta

$$x = a_n \cdot 10^n + \dots + a_1 \cdot 10 + a_0 \equiv (-1)^n \cdot a_n + \dots + a_2 - a_1 + a_0;$$

Cioè: un numero è divisibile per 11 (cioè è congruo a 0 modulo 11) se è divisibile per 11 la somma delle sue cifre prese con segno alternato.

Per esempio $x = 19679$ è divisibile per 11: infatti $1 - 9 + 6 - 7 + 9 = 0$ (ricordiamo che 0 è multiplo di qualunque numero); anche 81939 è divisibile per 11, poiché $8 - 1 + 9 - 3 + 9 = 22$.

Invece 2581 non è divisibile per 11: $-2 + 5 - 8 + 1 = -4$, è un numero della forma $11k - 4$, o, meglio, $11k + 7$.

Il criterio di divisibilità per 7 è più complesso.

Utilizzando le congruenze modulo 7 risulta:

$$10^0 \equiv 1 \pmod{7}$$

$$10^1 \equiv 3 \pmod{7};$$

calcolando le successive potenze di entrambi i membri:

$$10^2 \equiv 2 \pmod{7}$$

$$10^3 \equiv -1 \pmod{7}$$

$$10^4 \equiv -3 \pmod{7}$$

$$10^5 \equiv -2 \pmod{7}$$

$$10^6 \equiv 1 \pmod{7}$$

...

Le successive potenze di 10 ripetono periodicamente la stessa sequenza:

$$1, 3, 2, -1, -3, -2.$$

Dunque x è divisibile per 7 se

$$x = a_0 + a_1 10 + a_2 10^2 + \dots$$

$$\equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - \dots$$

$$= (a_0 - a_3 + a_6 - \dots) + 3(a_1 - a_4 + a_7 - \dots) + 2(a_2 - a_5 + a_8 - \dots) \equiv 0 \pmod{7}$$

Per esempio

$$3125486 \equiv (6 - 5 + 3) + 3(8 - 2) + 2(4 - 1) = 4 + 18 + 6 = 28 \equiv 0 \pmod{7}.$$

Dagli esempi svolti risulta chiaro che si può cercare un criterio di divisibilità per qualsiasi numero. Un metodo generale è il seguente: siano r_0, r_1, r_2, \dots i resti della divisione di $10^0, 10^1, 10^2, \dots$ per un certo numero d ; dette $a_0, a_1, a_2, \dots, a_n$ le cifre di x , risulta

$$x \equiv r_0 a_0 + r_1 a_1 + r_2 a_2 + \dots + r_n a_n.$$

Allora x è divisibile per d se

$$r_0 a_0 + r_1 a_1 + r_2 a_2 + \dots + r_n a_n \equiv 0 \pmod{d}.$$

Si noti che la successione dei resti è periodica, dato che i resti non nulli della divisione per d possono essere al più $d - 1$, e si possono quindi raggruppare opportunamente le cifre.

ESERCIZIO. Ricavare un criterio di divisibilità per 17.

Il metodo sopra indicato non è più conveniente se la successione dei resti che si ripetono è troppo lunga; per esempio, se vogliamo applicarla a 19, otteniamo una sequenza di 18 resti. Possiamo allora usare un altro metodo. Poiché $20 \equiv 1 \pmod{19}$, scriviamo il numero x del quale vogliamo valutare la divisibilità per 19 mettendo in evidenza il numero delle decine:

$$x = 10n + a_0;$$

x è divisibile per 19 se lo è il suo doppio:

$$2x = 20n + 2a_0.$$

Questa affermazione si basa sul seguente teorema, che è una diretta conseguenza del teorema fondamentale dell'aritmetica.

TEOREMA. Se a divide bc e $\text{MCD}(a, b) = 1$ allora a divide c .

Dimostrazione. Siano $b = b_1 b_2 \dots b_h$ e $c = c_1 c_2 \dots c_k$ le due scomposizioni (uniche) di b e c in fattori primi (non necessariamente distinti). Allora

$$bc = b_1 b_2 \dots b_h c_1 c_2 \dots c_k.$$

Se a divide bc tutti i fattori primi di a compaiono nella scomposizione di bc ; poiché a non può avere per ipotesi fattori comuni con b , tutti i fattori di a compaiono nella scomposizione di c , quindi a divide c .

Nel nostro caso: se 19 è un divisore di $2x$, poiché $\text{MCD}(19, 2) = 1$, allora 19 divide x .

divisibilità per 19

Ma $20 \equiv 1 \pmod{19}$, perciò

$$2x = 20n + 2a \equiv n + 2a \pmod{19}.$$

Concludendo, x è divisibile per 19 se lo è la somma delle sue decine e del doppio delle unità.

Per esempio, valutiamo la divisibilità per 19 di 7353:

$$7353 = 735 \cdot 10 + 3 \equiv 735 + 2 \cdot 3 = 741.$$

Quindi 7353 è divisibile per 19 se e solo se lo è 741: abbiamo diminuito di 1 cifra il numero da valutare; proseguiamo:

$$741 \equiv 74 + 2 = 76$$

$$76 \equiv 7 + 12 = 19,$$

quindi 7353 è divisibile per 19.

ESERCIZI

A. Trovare un criterio di divisibilità per 39.

B. Osservando che $50 \equiv 1 \pmod{7}$, stabilire un diverso criterio di divisibilità per 7.

Divagazione: Le equazioni diofantee e il teorema di Fermat.

Estendiamo a \mathbb{Z} la definizione di massimo comune divisore ponendo

$$\text{MCD}(a, b) = \text{MCD}(|a|, |b|).$$

Abbiamo visto come sia possibile utilizzare l'algoritmo euclideo per il calcolo di $\text{MCD}(a, b)$. Esso consiste nel calcolare il resto r_1 della divisione di a per b , e poiché ogni divisore comune di a e di b è anche divisore comune di b e r_1 , si prosegue, calcolando il resto r_2 tra b e r_1 , poi il resto r_3 tra r_1 e r_2 , e così via. Poiché

$$b > r_1 > r_2 > r_3 > \dots$$

necessariamente si arriverà (al più in b passaggi) ad avere resto 0. Se r_n è l'ultimo resto diverso da 0 allora

$$r_n = \text{MCD}(a, b).$$

I successivi passaggi possono essere indicati dalle seguenti uguaglianze:

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$r_2 = q_4 r_3 + r_4$$

...

$$r_{n-1} = q_n r_n + r_n$$

$$r_{n-1} = q_{n+1} r_n + 0.$$

Dimostriamo ora il seguente

TEOREMA. Se $d = \text{MCD}(a, b)$ allora d si può esprimere come *combinazione lineare* di a e b , cioè esistono $h, k \in \mathbb{Z}$ tali che

$$ha + kb = d.$$

Dimostrazione. Applichiamo l'algoritmo euclideo partendo dalla coppia di numeri a, b , fino a trovare l'ultimo resto r_n diverso da 0; dalla successione di uguaglianze sopra scritte abbiamo:

$$r_1 = a - q_1b,$$

cioè r_1 si può esprimere come combinazione lineare di a e b , con coefficienti $h = 1$ e $k = -q_1$;

$$r_2 = b - q_2(a - q_1b) = (1 + q_2q_1)b - q_2a,$$

cioè r_2 si può esprimere come combinazione lineare di a e b , con coefficienti $h = 1 + q_2q_1$ e $k = -q_2$; proseguendo in questo modo si arriva a esprimere ogni r_i come combinazione lineare di a e b , e quindi anche r_n :

$$r_n = ha + kb;$$

ma $r_n = \text{MCD}(a, b) = d$, da cui la tesi.

Per esempio, se $a = 64, b = 24$, allora $\text{MCD}(64, 24) = 8$; seguendo lo schema della dimostrazione si ottiene

$$8 = (-1) \cdot 64 + 3 \cdot 24,$$

Abbiamo visto che il numero $d = \text{MCD}(a, b)$ si può esprimere come combinazione lineare di a e b . Generalizziamo: quali sono *tutti* i numeri interi che si possono esprimere come combinazione lineare di a, b ?

In altre parole, il problema proposto corrisponde alla ricerca delle soluzioni intere della equazione

$$ax + by = c.$$

In generale qualunque equazione algebrica a coefficienti interi, della quale si ricerchino soltanto le soluzioni intere, viene detta *equazione diofantea*, dal nome del matematico greco Diofanto (III sec. d.C.) che se ne occupò nella sua *Aritmetica*. L'ultimo teorema di Fermat, ad esempio, prende in esame la risoluzione della equazione diofantea

$$x^n + y^n = z^n.$$

L'equazione lineare $ax + by = c$ è la più semplice equazione diofantea, ed è lo strumento per la risoluzione di quei problemi in cui si chiede di esprimere un certo numero come combinazione lineare di altri due, cioè come somma di loro opportuni multipli interi.

Sia A l'insieme che contiene tutti e soli i numeri che si possono esprimere come combinazione lineare di $a, b \in \mathbb{Z}$:

$$A = \{xa + yb : x, y \in \mathbb{Z}\};$$

sappiamo, per il teorema precedente, che se $d = \text{MCD}(a, b)$ allora $d \in A$.

Inoltre qualunque multiplo intero di d appartiene ad A : infatti se

$$d = ha + kb$$

allora

$$nd = (nh)a + (nk)b.$$

Viceversa, ogni elemento di A è un multiplo di d ; infatti se d è un divisore sia di a che di b , cioè $a = h_1d, b = h_2d$, allora d è un divisore di qualunque combinazione lineare di a e b :

$$xa + yb = (xh_1 + yh_2)d.$$

La conclusione è che A coincide con i multipli interi di d . Cioè: i numeri che si possono esprimere come combinazione lineare di a e b sono tutti e soli i multipli interi di $\text{MCD}(a, b)$.

In particolare, se $\text{MCD}(a, b) = 1$ (cioè se a e b sono primi tra loro), allora qualunque numero intero si può esprimere come combinazione lineare di a e b (infatti qualunque numero intero è multiplo di 1).

Quanto abbiamo finora esposto può essere riassunto dal seguente

TEOREMA. Condizione necessaria e sufficiente affinché l'equazione $ax + by = c$ (con $a, b, c \in \mathbb{Z}$) ammetta soluzioni intere è che c sia un multiplo di $\text{MCD}(a, b)$.

ESEMPIO 1. L'equazione $6x + 9y = 19$ non ammette soluzioni intere: poiché $\text{MCD}(6, 9)=3$, si possono esprimere come combinazione lineare di 6 e 9 tutti e soli i multipli di 3, quindi non 19. Si osservi che ciò è equivalente ad affermare che la retta di equazione $6x + 9y = 19$ non passa per alcun punto di coordinate intere.

ESEMPIO 2. L'equazione $5x + 7y=10$ ammette soluzioni intere, dato che 5 e 7 sono primi tra loro; ad esempio $x = 9$ e $y = -5$.

Abbiamo dunque risolto il problema di stabilire quando l'equazione diofantea $ax + by = c$ ammette soluzioni. Dobbiamo ancora determinare quante e quali sono le soluzioni quando esse esistono. Per arrivare a questo risultato dimostriamo un teorema che abbiamo già preannunciato, e cioè che in \mathbb{Z}_n sono invertibili solo gli elementi $[a]$ tali per cui a è primo con n .

TEOREMA. Un elemento $[a] \in \mathbb{Z}_n$ ammette l'inverso (rispetto al prodotto) se e solo se risulta $\text{MCD}(a, n)=1$.

Dimostrazione. Supponiamo per semplicità che il rappresentante a di $[a] \in \mathbb{Z}_n$ sia compreso tra 0 e n : $0 < a < n$; $\text{MCD}(a, n)$ non dipende dal rappresentante a dell'elemento $[a]$.

Infatti un rappresentante di $[a]$ è un numero intero della forma $a + hn$: poiché

$$\text{MCD}(x, y) = \text{MCD}(y, x \bmod y)$$

allora $\text{MCD}(n, a + hn) = \text{MCD}(n, a)$.

Ci chiediamo se esiste $[a'] \in \mathbb{Z}_n$ tale che

$$[a] \cdot [a'] = [1].$$

Quest'ultima relazione è equivalente alla seguente congruenza:

$$a \cdot a' \equiv 1 \pmod{n};$$

tale congruenza è a sua volta equivalente alla equazione

$$aa' - 1 = kn,$$

cioè

$$aa' - kn = 1.$$

Questa è una equazione diofantea con incognite a' e k , che, come abbiamo dimostrato, ammette soluzione in \mathbb{Z}_n se e solo se $\text{MCD}(a, n) = 1$. Se (a', k) è una soluzione qualsiasi allora

$$aa' \equiv 1 \pmod{n};$$

quindi $[a']$ è l'inverso di $[a]$ in \mathbb{Z}_n .

Da questo teorema deduciamo le seguenti immediate conseguenze.

1. In \mathbb{Z}_p , con p primo, ogni elemento diverso da $[0]$ ammette inverso ($[0]$ non ammette inverso poiché $\text{MCD}(p, 0) = p$).
2. In \mathbb{Z}_p , con p primo, non ci sono divisori dello zero, cioè non esistono $[a], [b] \in \mathbb{Z}_p$, entrambi diversi da $[0]$, tali che

$$[a] \cdot [b] = [0]$$

Infatti, moltiplicando per l'inverso $[a']$ di $[a]$ otterremmo

$$[a'] \cdot [a] \cdot [b] = [a'] \cdot [0]$$

$$[b] = [0],$$

contro l'ipotesi.

3. In \mathbb{Z}_n , con p primo, vale la legge di cancellazione del prodotto: se $[a] \cdot [b] = [a] \cdot [c]$ e $[a] \neq [0]$ allora $[b] = [c]$. In altre parole, se $ab \equiv ac \pmod{p}$, e $a \neq 0 \pmod{p}$ allora $b \equiv c \pmod{p}$.
4. In \mathbb{Z}_n , se n non è primo, allora la legge di cancellazione vale se e solo se l'elemento a che si "cancella" è invertibile in \mathbb{Z}_n , cioè se e solo se $\text{MCD}(a, n) = 1$.

ESEMPIO 3. In \mathbb{Z}_6 gli unici elementi che ammettono inverso sono $[1]$, che è ovviamente sempre inverso di se stesso, e $[5]$, il cui inverso è $[5]$:

$$[5] \cdot [5] = [1].$$

In \mathbb{Z}_6 esistono divisori dello zero: per esempio $[3] \cdot [4] = [0]$. Inoltre in \mathbb{Z}_6 non vale in generale la legge di cancellazione del prodotto: per esempio, $[4] \cdot [2] = [4] \cdot [5]$, ma $[2] \neq [5]$. In \mathbb{Z}_7 invece *tutti* gli elementi diversi da $[0]$ hanno l'inverso:

$$\begin{aligned} [1] \cdot [1] &= [1] \\ [2] \cdot [4] &= [1] \\ [3] \cdot [5] &= [1] \\ [6] \cdot [6] &= [1] \end{aligned}$$

e non esistono divisori dello zero.

Il precedente teorema ci offre la possibilità di risolvere l'equazione diofantea $ax + by = c$, con $a, b, c \in \mathbb{Z}$. Sappiamo che l'equazione ammette soluzioni intere se e solo se c è un multiplo di $\text{MCD}(a, b)$. Quindi possiamo supporre $\text{MCD}(a, b) = 1$: in caso contrario si dividono entrambi i membri dell'equazione per $\text{MCD}(a, b)$. L'equazione

$$ax + by = c$$

è equivalente all'equazione

$$(1) \quad ax - c = -by;$$

e quest'ultima uguaglianza dice che (x, y) è una soluzione dell'equazione data se e solo se $ax - c$ è multiplo di b , cioè se e solo se

$$ax \equiv c \pmod{b}.$$

Poiché per ipotesi $\text{MCD}(a, b) = 1$, esiste in \mathbb{Z}_b l'inverso $[a']$ di $[a]$; moltiplicando ambo i membri per a'

$$a'ax \equiv a'c \pmod{b};$$

ma $a'a \equiv 1 \pmod{b}$, dunque

$$x \equiv a'c \pmod{b}.$$

I corrispondenti valori di y si ricavano, per ogni x , dalla (1).

Quindi se una equazione diofantea lineare ammette soluzioni, queste sono infinite.

ESEMPIO 4. Risolvere l'equazione diofantea $5x + 7y = 24$.

Ricaviamo la congruenza

$$5x \equiv 24 \pmod{7}$$

cioè

$$5x \equiv 3 \pmod{7}.$$

In \mathbb{Z}_7 l'inverso di $[5]$ è $[3]$, dunque moltiplicando ambo i membri per 3 si ottiene

$$15x \equiv 9 \pmod{7}$$

cioè

$$x \equiv 2 \pmod{7}.$$

Le soluzioni per l'incognita x sono tutti e soli i numeri interi della forma $x = 2 + 7k$; sostituendo $x = 2 + 7k$ nell'equazione $5x + 7y = 24$ otteniamo $y = 2 - 5k$. Concludendo: per ogni $k \in \mathbb{Z}$ dalle equazioni

$$x = 2 + 7k$$

$$y = 2 - 5k$$

si ottengono le infinite soluzioni dell'equazione data:

$$\dots, (-12, 12), (-5, 7), (2, 2), (9, -3), (16, -8), \dots$$

ESERCIZIO. Risolvere l'equazione diofantea $6x + 7y = 2$.

Quindi la risoluzione di una equazione diofantea $ax + by = c$ è basata sulla determinazione dell'inverso di $[a]$ in \mathbb{Z}_b . Nel caso che b sia primo, il problema è risolto in modo molto brillante da un celebre teorema di Fermat.

Il Teorema di Fermat.

Il seguente teorema, enunciato dal matematico francese Pierre de Fermat (1601 – 1665) è di notevole importanza.

TEOREMA. Se p è primo, e a non è un multiplo di p , allora

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dimostrazione. I numeri $1, 2, 3, \dots, p-1$ sono, a due a due, non congrui modulo p . Di conseguenza anche i numeri

$$a, 2a, 3a, \dots, (p-1)a$$

sono, a due a due, non congrui modulo p , (e quindi coincidono, a meno dell'ordine, con $1, 2, 3, \dots, p-1$); infatti se fosse $ha \equiv ka \pmod{p}$, con $0 < h < p$, $0 < k < p$, $h \neq k$, allora, poiché $\text{MCD}(a, p) = 1$, varrebbe la legge di cancellazione per il prodotto, e risulterebbe

$$h \equiv k \pmod{p}$$

cioè $h = k$, contro l'ipotesi. Quindi

$$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$$

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}$$

e poiché $(p-1)!$ non è multiplo di p vale la legge di cancellazione, e risulta

$$a^{p-1} \equiv 1 \pmod{p}.$$

ESEMPIO 5. Se $p = 7$, allora per qualunque a , con $a \not\equiv 0 \pmod{7}$, risulta

$$a^6 \equiv 1 \pmod{7}.$$

Ad esempio:

$$a = 2: 2^6 = 64 \equiv 1 \pmod{7}$$

$$a = 3: 3^6 = 27 \cdot 27 \equiv 6 \cdot 6 \equiv 1 \pmod{7}$$

$$a = 5: 5^6 = 25^3 \equiv 4^3 = 64 \equiv 1 \pmod{7}.$$

Questo teorema ci offre una informazione importante sull'inverso di $[a] \neq [0]$ in \mathbb{Z}_p . Infatti, poiché

$$a^{p-1} = a \cdot a^{p-2}$$

possiamo scrivere

$$a \cdot a^{p-2} \equiv 1 \pmod{p}$$

cioè $[a^{p-2}]$ è l'inverso di $[a]$.

L'algoritmo che sfrutta il teorema di Fermat è il seguente:

Algoritmo per il calcolo dell'inverso di $[a]$ in \mathbb{Z}_p

leggi (p)

leggi (a)

$b := 1$

per $i := 1$ fino a $p-2$ fai

$b := (b \cdot a) \pmod{p}$

scrivi (b)

ESERCIZIO

Calcolare l'inverso di $[6]$ in \mathbb{Z}_{11} e in \mathbb{Z}_{13} ; risolvere quindi le equazioni diofantee

$$6x + 13y = 11$$

e

$$6x + 11y = 11$$

ESERCIZI DI RICAPITOLAZIONE:

1. Completare le seguenti uguaglianze:

- $3 \equiv 10 \pmod{\quad}$;
- $7 \equiv \quad \pmod{12}$;
- $-24 \equiv 3 \pmod{\quad}$;
- $\quad \equiv 8 \pmod{5}$;
- $28 \equiv 9 \pmod{\quad}$;

