ARITMETICA MODULARE

Teorema 14.2.1 (Algoritmo di divisione) *Siano $n, b \in \mathbb{N}$, $b \neq 0$. Allora esistono e sono unici due numeri interi q e r, detti rispettivamente quoziente e resto, tali che:*

$$n = qb + r \qquad \text{con} \quad 0 \leq r < b$$

Dimostrazione – Dimostriamo dapprima l'esistenza di q e r con il principio di induzione completa. $P(0)$ è vero in quanto $n = 0 = 0b + 0$, con $q = r = 0$. Supponiamo che $P(j)$ sia vero per ogni j tale che $0 \leq j < k$ e vogliamo mostrare $P(k)$ (vogliamo, cioè verificare l'ipotesi 2. del principio di induzione completa). Se $k < b$ allora:

andiamo per induzione su n

$$k = 0b + k \qquad \text{con resto } r = k \quad 0 \leq k < b$$

dunque $P(k)$ è vero per $k < b$. Sia ora $k \geq b$. Poiché $0 \leq k - b < k$, applicando l'ipotesi induttiva a $k - b$, abbiamo:

$$k - b = q_1 b + r_1 \qquad \text{con} \quad 0 \leq r_1 < b$$

da cui ricaviamo:

$$k = (q_1 + 1)b + r_1 \qquad \text{con} \quad 0 \leq r_1 < b$$

che dimostra quanto ci eravamo prefissati.

senza perdere di generalità,...

Mostriamo ora che q e r sono unici, e supponiamo che sia $n = q_1 b + r_1 = q_2 b + r_2$, con $0 \leq r_1 \leq r_2 < b$. Segue allora che $r_2 - r_1 = (q_1 - q_2)b$. Ora al primo membro dell'uguaglianza c'è un intero non negativo minore di b, al secondo membro c'è un multiplo di b, per cui devono essere entambi nulli, cioè $r_1 = r_2$ e $q_1 = q_2$. □

$\Rightarrow$ assurdo $\Rightarrow$

Teorema 14.2.8 (Identità di Bézout) *Siano a, b interi positivi e sia $d = \gcd(a, b)$. Allora esistono due numeri interi u, v (non unici) tali che:*

$$d = ua + vb$$

r, s si calcolano ripercorrendo all'indietro l'algoritmo di Euclide, 1 si ricavano i resti dall'uguaglianza precedente e 2 si sostituiscono, poi si raccoglie tutti i sottolineati

$$9 = 63 - 18 \cdot 3 = 63 - (270 - 63 \cdot 4) \cdot 3 =$$

$$= -270 \cdot 3 + 63 \cdot 13 = -270 \cdot 3$$

$$+ (603 - 270 \cdot 2) \cdot 13 = \text{raccolgo } 270$$

$$= \underbrace{-29}_{r} \cdot 270 + 603 \cdot \underbrace{13}_{s}$$

$\Rightarrow$ (segni sono sempre discordi)

Teorema 14.2.3 *Dati due interi a e b con $b \neq 0$, esiste un'unica coppia di interi p e q detti rispettivamente quoziente e resto tali che*

$$n = qb + r \qquad \text{con} \quad 0 \leq r < |b|$$

ove $|b|$ indica il valore assoluto di b.

interi $= \in \mathbb{Z}$

Definizione 14.2.4 Siano a e b due numeri interi. Diciamo che b *divide* a e scriviamo $b|a$, se esiste un numero intero c tale che $a = bc$. Diciamo che d è il *massimo comun divisore* tra due numeri a e b se li divide entrambi ed è il più grande numero intero con questa proprietà. Indicheremo il massimo comun divisore tra a e b con $\gcd(a, b)$.

$\text{mcd}(a,b) = (a,b) = \max\{d \text{ t.c. } d|a,\ d|b\}$

Teorema 14.2.6 (Algoritmo di Euclide) *Siano a e b due numeri interi positivi tali che $b \leq a$ e b non divide a. Abbiamo allora:*

$(-a,-b) = (a,b)$

$$\begin{aligned} a &= q_0 b + r_0 & \text{ove} \quad & 0 \leq r_0 < b \\ b &= q_1 r_0 + r_1 & \text{ove} \quad & 0 \leq r_1 < r_0 \\ r_0 &= q_2 r_1 + r_2 & \text{ove} \quad & 0 \leq r_2 < r_1 \\ &\vdots \\ r_{t-2} &= q_t r_{t-1} + r_t & \text{ove} \quad & 0 < r_t < r_{t-1} \\ r_{t-1} &= q_{t+1} r_t \end{aligned}$$

e l'ultimo resto non nullo r_t è il massimo comun divisore tra a e b.

Esempio 14.2.7

Vogliamo calcolare $\gcd(603, 270)$. Utilizziamo l'algoritmo di Euclide (Teorema 14.2.6).

$$603 = 2 \cdot 270 + 63 \qquad 63 = 603 - 270 \cdot 2 \qquad 270 > 63$$

$$270 = 4 \cdot 63 + 18 \qquad 18 = 270 - 63 \cdot 4 \qquad 63 > 18$$

$$63 = 3 \cdot 18 + 9 \qquad 9 = 63 - 18 \cdot 3 \qquad 18 > 9$$

$$18 = 2 \cdot 9$$

Dunque $\gcd(603, 270) = 9$.

Definizione 14.3.1 Siano a, b e n tre interi, con $n > 0$. Diciamo che a è *congruo* (o *congruente*) a b modulo n e scriviamo $a \equiv_n b$ se $n|a - b$.

La relazione di congruenza tra numeri interi verifica le seguenti proprietà:

(i) Proprietà riflessiva: $a \equiv_n a$, infatti $n|a - a = 0$.

(ii) Proprietà simmetrica: se $a \equiv_n b$ allora $b \equiv_n a$. Infatti, se $n|a - b$, allora $n|b - a$.

(iii) Proprietà transitiva: se $a \equiv_n b$ e $b \equiv_n c$ allora $a \equiv_n c$. Infatti, se $n|a - b$ e $n|b - c$, allora $n|a - b + b - c = a - c$.

$\equiv_n$ è una relazione di equivalenza

$a \equiv_n a$ sì perché $n | a - a = 0$ $\qquad 0 = 0 \cdot n$

$a \equiv_n b \Rightarrow n | a - b \Rightarrow n | b - a$

"se riesco a dividere -58 $\Rightarrow$ riesco a dividere anche 58" $\qquad 19 \equiv_{12} 7$

$\Rightarrow b \equiv_n a$

$b - a = -(a - b)$

$a \equiv_n b,\ b \equiv_n c \Rightarrow n | a - b,\ n | b - c$

se sommo due multipli di n ottengo un multiplo di n

$\Rightarrow n \,|\, (a-b) + (b-c) = a - c \qquad \Rightarrow a \equiv_n c$

l'insieme delle classi di equivalenza si dice l'insieme delle classi resto modulo n e si indica con $\mathbb{Z}_n$ ← finito

Definizione 14.3.3 Siano $a, n \in \mathbb{Z}$. Si chiama *classe di congruenza* di a modulo n e si indica con $[a]_n$ l'insieme di numeri interi congrui ad a modulo n:

infinito

$$[a]_n = \{b \in \mathbb{Z} \mid b \equiv_n a\} = \{a + kn \mid k \in \mathbb{Z}\}$$

$[a]_n = \{b \in \mathbb{Z} \text{ t.c. } b \equiv a \mod n\}$

$= \{b \in \mathbb{Z} \text{ t.c. } n | b - a\} = \{b \in \mathbb{Z} \text{ t.c. } (b - a) = kn, \text{ con } k \in \mathbb{Z}\}$

$= \{b \in \mathbb{Z} \text{ t.c. } b = a + kn, \text{ con } \mathbb{Z}\}$

$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}$ Definizione 2

Prop $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$

mostriamo che se $a \in \mathbb{Z}$ allora $[a]_n \in \{[0]_n, \dots, [n-1]_n\}$

Mostrare che tutti gli interi confluiscono in una di quelle $< n$

si scrive $a = nq + r$ $\quad 0 \le r < n$ $\Rightarrow nq = a - r$

$\Rightarrow n \mid a - r \Rightarrow a \equiv_n r \quad [a]_n = [r]_n$

Proposizione 14.3.6 devo prendere il resto 1

1. *Sia r il resto della divisione di a per n. Allora* $\boxed{[a]_n = [r]_n}$

2. $[0]_n, [1]_n, \dots, [n-1]_n$ *sono tutte e sole le classi di congruenza distinte modulo n;*

3. $[0]_n \cup [1]_n \cup \dots \cup [n-1]_n = \mathbb{Z}$.

resta da mostrare che se $0 \le i, j \le n-1$ $i \ne j$ allora $[i]_n \ne [j]_n$

Dim per negazione

$[i]_n = [j]_n \Rightarrow n \mid i - j$

possiamo supporre $i > j$ assurdo perché $0 < i - j < n$

quindi non può essere divisibile per n

Definizione 14.3.8 Definiamo sull'insieme $\mathbb{Z}_n$ le seguenti operazioni di somma e prodotto: 1

$$[a]_n + [b]_n = [a+b]_n \qquad [a]_n [b]_n = [ab]_n$$

Valgono associatività, commutatività e esistenza dell'elemento neutro per + e $\cdot$ e vale la distributività $([a]+[b])[c] = [a][c] + [b][c]$

~~Rispe~~ $[0]$ elemento neutro per +

$[1]$ " " " $\cdot$

esiste sempre l'opposto $[-a]$

non è detto che esista l'inverso

♦ **Osservazione 14.3.9** Le operazioni appena definite non dipendono dai numeri a e b che scegliamo per rappresentare le classi di congruenza che sommiamo o moltiplichiamo, ma soltanto dalla loro classe di congruenza. Si dice in tal caso che le operazioni sono *ben definite*. Per esempio, in $\mathbb{Z}_4$ si ha: $[1]_4 = [5]_4$ e $[2]_4 = [6]_4$. Per definizione $[1]_4 + [2]_4 = [3]_4 = [11]_4 = [5]_4 + [6]_4$. 1b

2

Dato $[a]_n \in \mathbb{Z}_n$ l'inverso di $[a]_n$ (se esiste) è un elemento $[b]_n \in \mathbb{Z}_n$ tale che $[a]_n [b]_n = [1]_n$. quindi viceversa l'inverso di $[b]$ è $[a]$

$[\frac{1}{3}]_5$ NON ha senso

$[1]_6 [2]_6 = [2]_6$

$[4]_6 [2]_6 = [2]_6$

2 in $[\cdot]_6$ non ha inverso

$[1][2] = [4][2]$ ma $[1] \ne [4]$

in $\mathbb{R}$ o $\mathbb{Q}$

$ab = cb$ e $b \ne 0 \Rightarrow a = c$

funziona perché (quando) b ha un inverso (infatti moltiplichiamo ambo i membri per il suo inverso $1/b$)

Esempio 14.3.10

Calcoliamo le tavole dell'addizione e della moltiplicazione per $\mathbb{Z}_3$ e $\mathbb{Z}_4$ invitando lo studente a esercitarsi a costruire le tavole analoghe per $\mathbb{Z}_5$ e $\mathbb{Z}_6$:

$\mathbb{Z}_3$

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

simmetrica rispetto alla diag.

$\cdot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

$[2 \cdot 6]$ $[6 \cdot 2]$

$\mathbb{Z}_4$

+	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$\cdot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

Notiamo alcuni fatti molto importanti: in $\mathbb{Z}_3$ ogni elemento diverso da $[0]_3$ ammette un *inverso*, cioè per ogni $[a]_3 \ne [0]_3$ esiste un elemento $[b]_3$ tale che $[a]_3[b]_3 = [1]_3$. Tale inverso si indica con $[a]_3^{-1}$. Abbiamo dunque: $[1]_3^{-1} = [1]_3$, $[2]_3^{-1} = [2]_3$. Tale proprietà invece non vale nel caso di $\mathbb{Z}_4$. Infatti la tavola moltiplicativa mostra che non esiste alcun inverso della classe $[2]_4$. Come vedremo dettagliatamente nel prossimo paragrafo, questa diversità è legata al fatto che 3 è un numero primo mentre 4 non lo è.

Proposizione 14.4.1 *Le seguenti affermazioni sono equivalenti:*

1) *p è un numero primo.* le cose succedono come nei reali (inverso + legge annullamento del prodotto)

2) *L'equazione $[a]_p x = [1]_p$, con $[a]_p \ne [0]_p$, ha soluzione in $\mathbb{Z}_p$, cioè ogni elemento $[a]_p \ne [0]_p$ in $\mathbb{Z}_p$ ammette inverso.*

3) *Se $[a]_p[b]_p = [0]_p$ in $\mathbb{Z}_p$ allora $[a]_p = [0]_p$ oppure $[b]_p = [0]_p$.*

Dimostrazione — 1) $\Longrightarrow$ 2): poiché $[a]_p \ne [0]_p$, p non divide a, quindi $\gcd(a,p) = 1$ (altrimenti sarebbe p). Allora per il Teorema 14.2.8 esistono $u, v \in \mathbb{Z}$ tali che $1 = au + pv$. Prendendo le classi di congruenza modulo p, abbiamo: $[1]_p = [a]_p[u]_p + \underbrace{[p]_p[v]_p}_{\text{è uguale a } 0} = [a]_p[u]_p$, dunque $x = [u]_p \in \mathbb{Z}_p$ è una soluzione di $[a]_p x = [1]_p$.

2) $\Longrightarrow$ 3): sia $[a]_p[b]_p = [0]_p$ con $[a]_p \ne [0]_p$. Per ipotesi esiste un inverso di $[a]_p$, cioè esiste un elemento $[u]_p$ tale che $[u]_p[a]_p = [1]_p$. Moltiplicando per $[u]_p$ entrambi i membri dell'uguaglianza $[a]_p[b]_p = [0]_p$ otteniamo: $\underbrace{[u]_p[a]_p}_{\text{è uguale a } 1}[b]_p = [u]_p[0]_p = [0]_p$, cioè $[b]_p = [0]_p$.

3) $\Longrightarrow$ 1): supponiamo che sia $p = ab$ e mostriamo che necessariamente a e b sono uguali a ± 1 o $\pm p$, cioè che gli unici divisori di p sono, a meno del segno, p stesso e 1. Osserviamo, considerando i valori assoluti, che $|a||b| = |ab| = |p| = p$ quindi $|a| \le p$ e $|b| \le p$. L'uguaglianza $p = ab$ si traduce in $\mathbb{Z}_p$ nell'uguaglianza $[p]_p = [a]_p[b]_p$, cioè $[a]_p[b]_p = [0]_p$. Per ipotesi sappiamo che $[a]_p = [0]_p$ oppure $[b]_p = [0]_p$. Se $[a]_p = [0]_p$, allora $a = \pm p$ e $b = \pm 1$. Se $[b]_p = [0]_p$, allora $b = \pm p$ e $a = \pm 1$. □

Proposizione 14.4.4 *La classe $[a]_n$ ammette un inverso in $\mathbb{Z}_n$ se e solo se* $\gcd(a,n) = 1$. è invertibile

$\Leftarrow$ RICETTA PER TROVARE L'INVERSO

Dim Per Bezout esistono r, s tali che $1 = ra + sn$, in $\mathbb{Z}_n$ abbiamo

$[1] = [ra]_n + [sn]_n = [r]_n[a]_n + [0]_n$

$\Rightarrow [r]_n$ è l'inverso di $[a]_n$

Viceversa Sia $[a] \in \mathbb{Z}_n$ e sia $[b]_n$ tale che $[a]_n[b]_n = [1]_n$

$\Rightarrow [ab]_n = [1]_n \Rightarrow n \mid ab - 1$

$\Rightarrow ab - 1 = nk \quad 1 = ab - nk$

Sia $d = (a, n) \quad d \mid a \quad d \mid n$

$d \mid ab - nk = 1 \Rightarrow d = 1$

un multiplo di d − un multiplo di d è ancora un multiplo di d

def interi coprimi: gli interi a e b si dicono coprimi (o primi tra loro o relativamente primi) sse essi non hanno nessun divisore comune eccetto 1 e -1 o, in modo equivalente, se il loro MCD è 1.

Esercizio 0 mai invertibile v 1

in $\mathbb{Z}_{20}$ gli elementi invertibili sono

$[1]_{20}$, $[3]_{20}$, $[7]_{20}$, $[9]_{20}$

$[11]_{20}$ $[13]_{20}$ $[17]_{20}$ $[19]_{20}$

Corollario p primo $[a] \in \mathbb{Z}_p$ $[a] \neq [0]$

$\Rightarrow [a]$ è invertibile

Dim $[a]_p \neq [0]_p \Rightarrow p \nmid a$

$\Rightarrow mcd(a,p) = 1 \Rightarrow [a]_p$ è invertibile

Proposizione 14.4.3 *Se* $\gcd(a,n) = 1$ *l'equazione* $[a]_n\, x = [b]_n$ *ha un'unica soluzione in* $\mathbb{Z}_n$.

Dimostrazione – Poiché $\gcd(a,n) = 1$, per il Teorema 14.2.8 esistono $s, v \in \mathbb{Z}$ tali che $as + nv = 1$, dunque $[a]_n$ è invertibile in $\mathbb{Z}_n$, con inverso $[s]_n$.

Otteniamo $[s][a]x = [s][b]$

$\Rightarrow x = [b]_n[s]_n = [bs]_n$

Prop l'equazione $[a]_m x = [b]_m$ ha soluzione in $\mathbb{Z}_m$ se e solo se $mcd(a,m)$ divide b e in tal caso ci sono esattamente d soluzioni, ove $d = mcd(a,m)$

Congruenze Trovare le soluzioni di $ax \equiv_n b$ significa trovare tutti gli interi z tal che $az \equiv_n b$

trasformiamo in un'eq in $\mathbb{Z}_n$

cioè $[a]_n[z]_n = [b]_n$ intesa come una classe

$\Rightarrow$ Ci sono infiniti soluzioni o nessuna soluzione

e.g. $3x \equiv_5 2$ $\quad [3]_5[x] = [2]_5$

$mcd(3,5) = 1$ $\Rightarrow 1$ sol in $\mathbb{Z}_m$ $\quad [3]$ è invertibile e il suo inverso è $[2]$ (tabella di prima)

$[2][3][x] = [2][2]$

$\Rightarrow [x]_5 = [4]_5$

$x = 4 + 5k$ con $k \in \mathbb{Z}$

Esercizio Trovare le soluzioni intere dell'equaz

$23x \equiv_{102} 12$ $\quad$ Risolviamo $[23]_{102}[x]_{102} = [12]_{102}$

Nota: ci sono soluz $\Leftrightarrow mcd(23,102)$ divide 12 (sappiamo già che è 1 perché 23 è primo)

$102 = 23 \cdot 4 + 10$

$23 = 10 \cdot 2 + 3$

$10 = 3 \cdot 3 + 1$ $\leftarrow mcd(102, 23) = 1$

$3 = 1 \cdot 3 + 0$

ordine inverso nelle sostituzioni

$10 = 102 - 23 \cdot 4$

$3 = 23 - 10 \cdot 2$ algo dove ricaviamo i resti

$1 = 10 - 3 \cdot 3$

$1 = 10 - 3 \cdot 3 = 10 - 3(23 - 10 \cdot 2) = 7 \cdot 10 - 3 \cdot 23$

$= 7(102 - 23 \cdot 4) - 3 \cdot 23 =$

$= 7 \cdot 102 - 31 \cdot 23$

$[1]_{\text{modulo } 102} = [7][102]_{102} - [31][23]_{102}$, $[102]_{102} = [0]$

l'inverso di $[23]$ è $[-31]$

$[23][-31] = [1]$ $\quad [23][x] = [12]$

$[-31][23][x] = [12][-31]$

$[x]_{102} = [12]_{102}[-31]_{102} = [-372]_{102} = [-66]_{102}$ $\quad (-372 = -306 - 66)$

$x = -372 + k\, 102$ con $k \in \mathbb{Z}$

$(x = -66 + k\, 102$ con $k \in \mathbb{Z})$

Esercizio

consideriamo

$[32]_{24}$ e $[-88]_{48}$

sono $=$? sono $\neq$? $[32]_{24} \subseteq [-88]_{48}$?

$[-88]_{48} \subseteq [32]_{24}$?

$[32]_{24} = [8]_{24} = 8 + 24K \quad K \in \mathbb{Z}$

$[-88]_{48} = [8]_{48} = 8 + 48K \quad K \in \mathbb{Z}$

abbiamo $[8]_{48} \subseteq [8]_{24}$

perché se $z \in [8]_{48}$

$z = 8 + 48K = 8 + (2K)24$

quindi $[-88]_{48} \subseteq [32]_{24}$