G. PARMEGGIANI 28/2/2019

ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)
Corso di Laurea: Informatica

Ritorniamo alla divisione in $\mathbb{Z}$

Se $a, b \in \mathbb{Z}$ e $d = MCD(a,b)$, vogliamo trovare $m, n \in \mathbb{Z}$ tali che

$$d = ma + nb$$

ESEMPIO $\quad a = 10$, $b = 4$

Calcolando d con l'algoritmo di Euclide otteniamo:

$$\underbrace{10}_{a} = \underbrace{4}_{b} \cdot \underbrace{2}_{q_1} + \underbrace{2}_{r_1}$$

$$\underbrace{4}_{b} = \underbrace{2}_{r_1} \cdot \underbrace{2}_{q_2} + \underbrace{0}_{r_2}$$

$\Rightarrow d = MCD(a,b) = r_1$ e $\quad \underbrace{2}_{d = r_1} = \underbrace{10}_{a} \cdot \overset{m}{1} + \underbrace{4}_{b} \cdot \overset{n}{(-2)}$

N.B. m ed n non sono univocamente individuati

$$\underbrace{2}_{d = MCD(a,b)} = \underbrace{10}_{a} \cdot 3 + \underbrace{4}_{b} \cdot (-7)$$

quando $a = 10$, $b = 4$

(in questo caso potrei prendere anche $m = 3$ ed $n = -7$)

TEOREMA (IDENTITA' DI BEZOUT)

$\forall a, b \in \mathbb{Z}$, posto $d = MCD(a,b)$, $\exists\, m, n \in \mathbb{Z}$ tali che

$$d = m \cdot a + n \cdot b$$

N.B m ed n non sono unici (esempio all'inizio della lezione)

Per trovare m ed n posso:

① Applicare l'algoritmo di Euclide in $\mathbb{Z}$ e ripercorrerlo a ritroso

oppure (se a e b non sono entrambi positivi)

② $\boxed{I}$ Calcolare $|a|, |b| \in \mathbb{N}$

$\boxed{II}$ osservare che $MCD(a,b) = MCD(|a|,|b|)$

$\boxed{III}$ se d è il massimo comun divisore positivo di $|a|$ e $|b|$, calcolare d con l'algoritmo di Euclide in $\mathbb{N}$, e poi, ripercorrendolo a ritroso, trovare $m^*, n^* \in \mathbb{Z}$ tali che

$$d = m^* \cdot |a| + n^* \cdot |b|$$

$\boxed{IV}$ Dalla relazione $d = m^*|a| + n^*|b|$ posso trovare $m, n \in \mathbb{Z}$ tali che $d = ma + nb$ "aggiustando i segni" di m^* ed n^*

ESEMPIO Sia d il massimo comun divisore positivo di $a = -36$ e $b = 28$

Trovare $m, n \in \mathbb{Z}$ tali che $d = ma + nb$.

$\boxed{1^\circ \text{ modo}}$ Uso l'algoritmo di Euclide in $\mathbb{Z}$:

① $\underset{a}{-36} = \underset{b}{28} \cdot \underset{q_1}{(-2)} + \underset{r_1}{20}$

② $\underset{b}{28} = \underset{r_1}{20} \cdot \underset{q_2}{1} + \underset{r_2}{8}$

③ $\underset{r_1}{20} = \underset{r_2}{8} \cdot \underset{q_3}{2} + \underset{r_3}{4}$

④ $\underset{r_2}{8} = \underset{r_3}{4} \cdot \underset{q_4}{2} + \underset{r_4}{0}$

③+④ $\Rightarrow$ $d = 4 = 20 - 8 \cdot 2 = 20 - (28-20) \cdot 2 =$

$\boxed{② \Rightarrow 8 = 28 - 20}$

$= 20 - 28 \cdot 2 + 20 \cdot 2 = 20 \cdot 3 - 28 \cdot 2 = (-36 + 28 \cdot 2) \cdot 3 - 28 \cdot 2$

$\boxed{① \Rightarrow 20 = -36 + 28 \cdot 2}$

$= -36 \cdot 3 + 28 \cdot 6 - 28 \cdot 2 =$

$= -36 \cdot 3 + 28 \cdot 4$

$$\Rightarrow \quad \underset{d}{4} = \underset{a}{\underbrace{-36}} \cdot \underset{m}{3} + \underset{b}{28} \cdot \underset{n}{4}$$

2° MODO

$a = -36 \Rightarrow |a| = 36$

$b = 28 \Rightarrow |b| = 28$

Uso l'algoritmo di Euclide in $\mathbb{N}$ per calcolare MCD$(|a|, |b|)$

① $\underset{|a|}{36} = \underset{|b|}{28} \cdot \underset{q_1}{2} + \underset{r_1}{8}$

② $\underset{|b|}{28} = \underset{r_1}{8} \cdot \underset{q_2}{3} + \underset{r_2}{4}$

③ $\underset{r_1}{8} = \underset{r_2}{4} \cdot \underset{q_3}{2} + \underset{r_3}{0}$

② + ③ $\Rightarrow d = 4 = 28 - 8 \cdot 3 = 28 - (36 - 28) \cdot 3 =$

$\boxed{① \Rightarrow 8 = 36 - 28}$

$= 28 - 36 \cdot 3 + 28 \cdot 3 = 28 \cdot 4 - 36 \cdot 3$

$d = m^* |a| + n^* |b|$ con $d = 4$, $|a| = 36$, $|b| = 28$, $m^* = -3$, $n^* = 4$

e quindi $d = ma + nb$ con $d = 4$, $a = -36$, $b = 28$, $m = 3$, $n = 4$

PER CASA: ESERCIZIO 4 (file: I19casaT1.pdf)

CLASSI DI CONGRUENZA

Def Siano $a, b \in \mathbb{Z}$
$n \in \mathbb{N}$
$n > 0$

Si dice che a è **CONGRUO** (o **CONGRUENTE**) a b **MODULO n**

se $n \mid (a-b)$

($\mid$ = divide)

Si scrive $a \equiv b \bmod n$ oppure $a \equiv b \pmod n$ oppure $a \equiv_n b$

NB1 $a \equiv b \bmod n \iff$ [il resto della divisione di a per n] = [il resto della divisione di b per n]

DIMOSTRAZIONE

Divido a per n: $a = nq_1 + r_1$ con $0 \le r_1 < n$

Divido b per n: $b = nq_2 + r_2$ con $0 \le r_2 < n$

"$\Longrightarrow$" IPOTESI: $a \equiv b \bmod n$

TESI: $r_1 = r_2$

DIM: Per ipotesi $a \equiv b \bmod n$, per cui $n \mid (a-b)$

Da $a - b = nq_1 + r_1 - (nq_2 + r_2) = n(q_1 - q_2) + (r_1 - r_2)$

$$\boxed{\begin{aligned} a &= nq_1 + r_1 \\ b &= nq_2 + r_2 \end{aligned}}$$

si ottiene: $r_1 - r_2 = (a-b) - n(q_1 - q_2)$

$$\left.\begin{aligned} &n \mid n(q_1 - q_1) \\ &\boxed{n \mid a-b} \end{aligned}\right\} \Rightarrow n \mid (a-b) - n(q_1 - q_2)$$

PERCHE' PER IPOTESI $a \equiv b \bmod n$

$\Rightarrow n \mid r_1 - r_2$ ed anche $n \mid r_2 - r_1$

Se $r_1 \ge r_2$ da $\begin{cases} 0 \le r_1 < n \\ 0 \le r_2 < n \end{cases}$ segue $0 \le r_1 - r_2 < n$, per cui

$n \mid r_1 - r_2$ implica $r_1 - r_2 = 0$ e quindi $r_1 = r_2$.

Analogamente, se $r_2 \geq r_1$, da $\begin{cases} 0 \leq r_1 < n \\ 0 \leq r_2 < n \end{cases}$ segue $0 \leq r_2 - r_1 < n$, per cui $n \mid r_2 - r_1$ implica $r_2 - r_1 = 0$ e quindi $r_2 = r_1$.

" $\Longleftarrow$ " IPOTESI: $r_1 = r_2$

TESI: $a \equiv b \mod n$

DIM:

$$\left.\begin{array}{l} a = nq_1 + r_1 \\ r_1 = r_2 \end{array}\right\} \Longrightarrow a = nq_1 + r_2 = nq_1 + b - nq_2$$

$$\boxed{b = nq_2 + r_2 \Rightarrow r_2 = b - nq_2}$$

$$\Longrightarrow \quad a - b = n(q_1 - q_2) \Longrightarrow n \mid (a-b) \Longrightarrow a \equiv b \mod n$$

PER CASA: ESERCIZIO 5 (file: I19casoT1.pdf)

$\boxed{\text{NB2}}$ Fissato $n \in \mathbb{N}$, $n > 0$, la relazione di congruenza modulo n gode delle seguenti proprietà:

$\boxed{1}$ È RIFLESSIVA: $a \equiv a \mod n \quad \forall a$ Infatti: $n \mid \underbrace{(a-a)}_{0}$

$\boxed{2}$ È SIMMETRICA: $a \equiv b \mod n \Longrightarrow b \equiv a \mod n$

Infatti: $n \mid (a-b) \Longrightarrow n \mid (b-a)$

$\boxed{3}$ È TRANSITIVA: $\left.\begin{array}{l} a \equiv b \mod n \\ b \equiv c \mod n \end{array}\right\} \Longrightarrow a \equiv c \mod n$

Infatti: $\left.\begin{array}{l} n \mid (a-b) \\ n \mid (b-c) \end{array}\right\} \Longrightarrow n \mid [(a-b) + (b-c)] = (a-c)$

Ogni relazione che gode delle proprietà $\boxed{1}$, $\boxed{2}$ e $\boxed{3}$ (tutte e tre) si dice una RELAZIONE DI EQUIVALENZA

Le relazioni di congruenza godono anche delle due seguenti proprietà (di cui non tutte le relazioni di equivalenza godono):

fissato $n \in \mathbb{N}$, $n > 0$, $a_1, a_2, b_1, b_2 \in \mathbb{Z}$

$\boxed{4}$ $\left.\begin{array}{l} a_1 \equiv b_1 \bmod n \\ a_2 \equiv b_2 \bmod n \end{array}\right\} \Rightarrow (a_1+a_2) \equiv (b_1+b_2) \bmod n$ LE CONGRUENZE MODULO n SI POSSONO SOMMARE

$\boxed{5}$ $\left.\begin{array}{l} a_1 \equiv b_1 \bmod n \\ a_2 \equiv b_2 \bmod n \end{array}\right\} \Rightarrow (a_1 \cdot a_2) \equiv (b_1 \cdot b_2) \bmod n$ LE CONGRUENZE MODULO n SI POSSONO MOLTIPLICARE

Def $a, n \in \mathbb{Z}$, $n > 0$, si chiama CLASSE DI CONGRUENZA DI a MODULO e si indica $[a]_n$ oppure $[a] \bmod n$

$[a]_n$ = insieme di tutti i numeri interi che sono congrui ad a modulo n =

$= \{ b \in \mathbb{Z} \mid b \equiv a \bmod n \}$

Dunque

$b \in [a]_n \underset{\text{def } [\,]_n}{\Longleftrightarrow} b \equiv a \bmod n \Longleftrightarrow r_2 = r_1 \Longleftrightarrow a = nq_1 + r_2 =$

PER IL NB 1 se $a = nq_1 + r_1$ e $b = nq_2 + r_2$ con $0 \leq r_1 < n$ e $0 \leq r_2 < n$

$r_2 = b - nq_2$

$= nq_1 + (b - nq_2) = b + n(q_1 - q_2)$

da cui $b = a + nk$ con $k = q_2 - q_1 \in \mathbb{Z}$

Viceversa, se $b = a + nk$ per un opportuno $k \in \mathbb{Z}$, allora $b - a = nk$ è divisibile per n per cui $b \equiv a \bmod n$

Abbiamo provato che:

$$\boxed{\begin{array}{l} [a]_n = \{ b \in \mathbb{Z} \mid b \equiv a \bmod n \} = \\ = \{ a + nk \mid k \in \mathbb{Z} \} \end{array}}$$

ESEMPIO 1 $n=2$

$a=0$ $[0]_2 = \{0+2\cdot k \mid k\in\mathbb{Z}\} = \{2k \mid k\in\mathbb{Z}\} =$ insieme dei numeri interi PARI

$a=1$ $[1]_2 = \{1+2k \mid k\in\mathbb{Z}\}$ = insieme dei numeri interi DISPARI

ESEMPIO 2 $n=4$

$[0]_4 = \{0+4k \mid k\in\mathbb{Z}\} = \{4k \mid k\in\mathbb{Z}\} = \{0,4,-4,8,-8,\dots\}$

$[1]_4 = \{1+4k \mid k\in\mathbb{Z}\} = \{1,5,-3,9,-7,\dots\}$

$[2]_4 = \{2+4k \mid k\in\mathbb{Z}\} = \{2,6,-2,10,-6,\dots\}$

$[3]_4 = \{3+4k \mid k\in\mathbb{Z}\} = \{3,7,-1,11,-5,\dots\}$

OSSERVAZIONE

$[4]_4 = [0]_4 = [-4]_4 = [8]_4 = [-8]_4 \dots$

$[5]_4 = [1]_4 = [-3]_4 = \dots$

$[6]_4 = [2]_4 = [-2]_4 = \dots$

$[7]_4 = [3]_4 = [-1]_4 = [11]_4 = [-5]_4 \dots$

IN GENERALE:

$\boxed{\text{I}}$ $\forall n\in\mathbb{N}, n>0, \quad \forall a,k\in\mathbb{Z}$

$[a]_n = [a+kn]_n$

$\boxed{\text{II}}$ Equivalentemente:

$c\in[a]_n \Rightarrow [a]_n = [c]_n$

$\boxed{\text{III}}$ In particolare, dividendo a per n:

$a = qn + r$ con $0\le r<n$

si ha: $[a]_n = [r]_n$

Def Ogni elemento di $[a]_n$ si chiama RAPPRESENTANTE della classe di congruenza di a modulo n

$\boxed{\text{NB 3}}$ Fissato n, non ci sono elementi in comune a due classi di congruenza (modulo n) diverse:

$\forall n, n>0, \forall a, b \in \mathbb{Z}$

siano $[a]_n$ e $[b]_n$ le classi di congruenza modulo n di rappresentanti a e b. Allora:

o $[a]_n = [b]_n$ (le due CLASSI sono UGUALI)

oppure $[a]_n \neq [b]_n$ (le due CLASSI sono DIVERSE).

Poiché abbiamo visto che

$[a]_n = \{a+nk \mid k \in \mathbb{Z}\}$ e $[b]_n = \{b+nk \mid k \in \mathbb{Z}\}$,

se $[a]_n \neq [b]_n$ allora

$\{a+nk \mid k \in \mathbb{Z}\} \cap \{b+nk \mid k \in \mathbb{Z}\} = \emptyset$

(ossia l'intersezione dei due insiemi di numeri interi è l'insieme vuoto. Si dice: "i due insiemi sono DISGIUNTI")

(Infatti: se esistesse un numero intero

$$c \in \underbrace{\{a+nk \mid k \in \mathbb{Z}\}}_{=[a]_n} \cap \underbrace{\{b+nk \mid k \in \mathbb{Z}\}}_{=[b]_n}$$

da $c \in [a]_n$ seguirebbe $[c]_n = [a]_n$,

e da $c \in [b]_n$ seguirebbe $[c]_n = [b]_n$.

Quindi si concluderebbe $[a]_n = [c]_n = [b]_n$, mentre stiamo supponendo $[a]_n \neq [b]_n$).

$\boxed{NB4}$ Fissato $n \in \mathbb{N}$, $n > 0$, l'UNIONE di tutte le classi di congruenza modulo n è $\mathbb{Z}$:

$$\bigcup_{0 \le a < n} [a]_n = \mathbb{Z}.$$

$\boxed{DEF.}$ L'insieme degli INTERI MODULO n, indicato con il simbolo $\mathbb{Z}_n$ è:

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

In $\mathbb{Z}_n$ si definiscono $+$ e $\cdot$ nel seguente modo:

$\forall [a]_n, [b]_n \in \mathbb{Z}_n$

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

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

$\boxed{NB}$ Se $a_1 \in [a]_n$ e $b_1 \in [b]_n$ $\Longrightarrow [a_1 + b_1]_n = [a+b]_n$

per cui la definizione di $+$ non dipende dalla scelta dei rappresentanti delle classi (ma solo dalle classi). Si dice che $+$ è "ben definita".

Analogamente:

se $a_1 \in [a]_n$ e $b_1 \in [b]_n$ $\Longrightarrow [a_1 \cdot b_1]_n = [a \cdot b]_n$

per cui la definizione di $\cdot$ non dipende dalla scelta dei rappresentanti delle classi (ma solo dalle classi).
Si dice che $\cdot$ è "ben definita".

TAVOLE DI ADDIZIONE E DI MOLTIPLICAZIONE - ESEMPI

$\mathbb{Z}_2 = \{[0]_2, [1]_2\}$

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

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

perché $[1]_2+[1]_2=[1+1]_2=[2]_2=[0]_2$

$\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$

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

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

N.B. in $\mathbb{Z}_4$ NON vale la LEGGE DI CANCELLAZIONE DEL PRODOTTO

PER CASA: ESERCIZIO 6 (file: I19casaT1.pdf)