ESERCITAZIONE N.5

6 novembre 2007

- Divisione euclidea in Z
- Algoritmo euclideo per la determinazione del M.C.D.
- Identità di Bezout
- Equazioni diofantee lineari

Rosalba Barattero

ESERCIZIO 1.

La relazione "divide" in Z

E' data in Z^* la corrispondenza $x \sim y \Leftrightarrow$ x divide y.

Stabilire se è riflessiva, simmetrica, transitiva.

Diciamo che x divide y e scriviamo $x|y$ se esiste $z \in Z^*$ tale che $y=xz$. Si può anche dire che x è un divisore di y, o che y è un multiplo di x.

Ad es. $2|12$ perché $12=2 \cdot 6$, $3 \nmid 8$ (3 non divide 8) perché non esiste nessun $z \in Z^*$ tale che $8=3z$.

RIFLESSIVA: a divide a ? Sì $a=1 \cdot a$

SIMMETRICA: Se $a|b$ allora $b|a$?

NO, 2 divide 12 ma 12 non divide 2

TRANSITIVA: Se $a|b$ e $b|c$ allora $a|c$?

Ipotesi : $a|b \Rightarrow \exists\, c \in Z^*$ t.c. $b=ac$ (1)

$b|c \Rightarrow \exists\, d \in Z^*$ t.c. $c=bd$ (2)

Tesi : $a|c$ cioè $\exists\, x \in Z^*$ t.c. $c=ax$

Da (2) $c=bd$, sostituendo (1) si ha : $c=(ac)d=a(cd)$.

Quindi $x=cd$ va bene. Perciò $\sim$ è transitiva.

LA DIVISIONE EUCLIDEA IN Z

Siano a, b $\in$ **Z** , $b\neq0$. Allora esistono e sono unici due interi, il quoziente q e il resto r tali che $a = b\cdot q + r$, con $0\leq r<|b|$.

Come si fa la divisione se entrambi o uno dei numeri a, b è negativo ?

<u>Esempio 1</u> : -62 : 20 = ?

-62 = 20 (-3) – 2 Non va bene ! il resto è negativo !

-62 = 20(-4) + 18 OK !

<u>Esempio 2</u>: 62 : (-20) = ?

Si fa 62 = 20 · 3 +2, poi si cambia segno …

62 = (-20) · (- 3) +2

<u>Esempio 3</u>: (-62) : (-20) = ?

(-62) = (-20) · 4 +18.

Vediamo un' applicazione dell'algoritmo della divisione.

ESERCIZIO 2.

Numeri di patente in Florida*

I numeri di patente in Florida sono codificati nel modo seguente SSSS-FFF-YY-DDD, dove nei gruppi con 'S' ed 'F' ci sono informazioni relative a nome e cognome, mentre YY indicano le ultime due cifre dell'anno di nascita e DDD codificano il mese m e il giorno b di nascita secondo la seguente espressione:

40(m-1)+b nel caso dei maschi,

40(m-1)+b+500 nel caso delle femmine.

Trascuriamo i casi di persone aventi lo stesso numero di patente, etc.

Determiniamo la data di nascita e il sesso dei titolari di patente aventi un numero di patente le cui ultime 5 cifre del codice sono: 80251, 62789.

80251: 80 indica l'anno di nascita 1980

251 corrisponde a 40(m-1)+b , poiché risulta $40(m-1)+b+500 \geq 501$. Si tratta quindi di maschio.

251 : 40 = ? 251= 40 · 6+11

6 è il quoziente e 11 il resto (univocamente determinati).

$\Rightarrow$ 80251 : maschio nato il giorno 11 luglio 1980

* Joseph Gallian – *Contemporary Abstract Algebra* – D.C. Heath and Company - 1994

62789: 62 indica l'anno di nascita 1962

789 corrisponde a 40(m-1)+b+500, poiché il massimo di 40(m-1)+b è $40 \cdot 11 + 31 = 471$. Si tratta quindi di femmina.

789= 40(m-1)+b+500 ⇒ 789-500= 40(m-1)+b

⇒ 289=40(m-1)+b

289 : 40 = ? $289= 40 \cdot 7+9$

7 è il quoziente e 9 il resto (univocamente determinati).

⇒ 62789 : femmina nata il giorno 9 agosto 1962.

Per approfondimenti su US Driver's License Numbers:

http://www.highprogrammer.com/alan/numbers/dl_us_shared.html

http://www.highprogrammer.com/alan/numbers/dl_us_shared_mmm.html

Qui un applet Java per codificare i dati della Florida

http://www.highprogrammer.com/cgi-bin/uniqueid/dl_fl

DEF. di M.C.D. (a,b) , con a, b interi non entrambi nulli:

è quell'intero d tale che

- d|a e d|b
- per ogni intero c tale che c|a e c|b, risulta c|d

Esempi :

- M.C.D. (12,18)= 6.

  L'insieme dei divisori comuni (positivi) è: {1,2,3,6},

  6 è il più grande dei divisori comuni, ed è anche multiplo di tutti i divisori.

  Anche -6 va bene, ma prendiamo quello positivo: intendiamo che in Z M.C.D. è unico a meno del segno.

- M.C.D. (10,0) = ? E' un caso particolare.

  Qualunque numero divide zero: $a \cdot 0=0\ \forall a \in Z$.

  {1,2,5,10} è l'insieme dei divisori comuni , 10 è il M.C.D.(10,0).

ESERCIZIO 3.

M.C.D. con l'algoritmo euclideo e identità di Bezout

Calcolare il M.C.D. tra 88 e 34 con l'algoritmo di Euclide, e scrivere la corrispondente identità di Bezout.

L'algoritmo euclideo consiste in una sequenza di divisioni successive:

1. $88 = 34 \cdot 2 + 20 \longrightarrow$ poiché il resto è $20 \neq 0$, procediamo dividendo il divisore 34 per il resto 20, e così via, fino ad avere resto nullo.
2. $34 = 20 \cdot 1 + 14$
3. $20 = 14 \cdot 1 + 6$
4. $14 = 6 \cdot 2 + 2$
5. $6 = 2 \cdot 3$

L'algoritmo di Euclide afferma che l'ultimo resto non nullo è il M.C.D.(88,34). Abbiamo ritrovato M.C.D.(88,34)=2 .

Questo succede perché il M.C.D. tra dividendo e divisore di una divisione euclidea è uguale al M.C.D. tra divisore e resto.
Così si ha: M.C.D.(88,34)=M.C.D.(34,20)=M.C.D. (20,14) = M.C.D.(14,6) = M.C.D.(6,2) = 2

Teorema di Bezout

Se d= M.C.D. (a,b), allora esistono due interi m, n tali che d= am +bn.

Scriviamo dunque 2 come combinazione lineare di 88 e 34, ossia cerchiamo due interi x e y tali che $88x + 34y = 2$.
Alla tabella precedente affianchiamo a destra l'espressione dei resti:

1. $88 = 34 \cdot 2 + 20$	$20 = 88 - 34 \cdot 2$
2. $34 = 20 \cdot 1 + 14$	$14 = 34 - 20 \cdot 1$
3. $20 = 14 \cdot 1 + 6$	$6 = 20 - 14 \cdot 1$
4. $14 = 6 \cdot 2 + 2$	$2 = 14 - 6 \cdot 2$
5. $6 = 2 \cdot 3$	

Partiamo dalla riga 4.(quella in cui compare l'ultimo resto non nullo), e sostituiamo a ritroso i resti:

$$2 = 14 - 6 \cdot 2$$
$$= 14 - (20 - 14 \cdot 1) \cdot 2 = 14 - 20 \cdot 2 + 14 \cdot 2 = 14 \cdot 3 - 20 \cdot 2$$
$$= (34 - 20 \cdot 1) \cdot 3 - 20 \cdot 2 = 34 \cdot 3 - 20 \cdot 3 - 20 \cdot 2 = 34 \cdot 3 - 20 \cdot 5$$
$$= 34 \cdot 3 - (88 - 34 \cdot 2) \cdot 5 = 34 \cdot 3 - 88 \cdot 5 + 34 \cdot 10 = 34 \cdot 13 - 88 \cdot 5$$
$$= 88\,(-5) + 34\,(13)$$

OK !

CONCLUSIONE. M.C.D.(88,34)=2 & $2 = 88(-5) + 34(13)$

Osservazione a) se n indica il n° dei passi dell'algoritmo euclideo si ha : $n \leq 2\lg_2 b$. Qui $n \leq 2\lg_2 34 \approx 2 \cdot 5.08 \leq 11$
b) Un'altra maggiorazione [G. Lamé]: **n ≤ 5m**, con m=n° cifre del minore tra i due numeri a e b. Qui **n≤ 5·2=10**

EQUAZIONI DIOFANTEE LINEARI

(= equazioni di I° grado a coefficienti
in **Z** che vengono risolte in **Z**)

1 INCOGNITA

Esempi a) $3x=4$ non ha sol. in **Z**

b) $5x=10$ ha unica sol. in **Z**, $x= 10/5 =2$

Quindi $ax=b$ con $a, b \in$ **Z** , $a\neq 0$ ha un'unica soluzione in Z ($x= b/a$) se e solo se $a|b$ (a divide b)

Altrimenti **non** ci sono **soluzioni in Z**

2 INCOGNITE

Esempi a) $4x+6y=3$ **non** ha sol. in **Z**:comunque si sostituiscano x e y con due interi il I° membro è pari, il secondo è dispari.
Si noti che in **R** l'equazione ha infinite soluzioni, basta assegnare ad x un generico valore reale t e ricavare il corrispondente

$y=\frac{3-4t}{6}$, con $t\in R$.

b) $3x+6y=18$ **ha** soluzioni intere,ad esempio (4,1), (-6,6),(10,-2).

c) $88x+34y=2$ ha tra le sue soluzioni (-5,13): trovate nell'es.prec.

PROBLEMA 1. Stabilire se e quando $ax+by=c$ ha soluzioni in **Z.**

[Osservazione. Se c=0 esiste almeno la soluzione (0,0).]

RISPOSTA L'equazione $ax+by=c$, con $a,b,c\in$ **Z***

ha soluzioni in **Z** ⇔ M.C.D. (a,b) divide c.

Dim. Se esiste la soluzione intera (x_0,y_0) allora si ha $ax_0+by_0=c$.
Se d è il M.C.D. (a,b) allora $a=dr$, $b=ds$, quindi sostituendo : $c= (dr)x_0+(ds)y_0 = d(rx_0+sy_0)$, che ci dice d divide c.
Viceversa supponiamo che d divida c, ossia $dm=c$.
Dalla proprietà del M.C.D.(a,b) si sa che esistono $x_0,y_0 \in$ **Z** tali che $d= ax_0+by_0$. Quindi si ha: $c = dm= (ax_0+by_0)m = a(mx_0)+b(my_0)$
Questo ci dice che l'equazione diofantea $ax+by=c$ ha la soluzione $x= mx_0$, $y=my_0$ (o meglio la coppia (mx_0,my_0)).

ESERCIZIO4. Stabilire se l'equazione lineare $88x+34y=10$ ha soluzioni intere.

Per l'Ex.3 M.C.D.(88,34)=2. Poiché 2 divide 10, l'equazione ha soluzioni intere, per il risultato precedente.

Ma possiamo dire di più : nell'Ex. 3 si era trovato

$88(-5) + 34(13) = 2$

Se moltiplichiamo l'uguaglianza per 5 troviamo:

$88(-5\cdot 5) + 34(13\cdot 5) = 2\cdot 5$, che possiamo trascrivere così

$88(-25) + 34(65) = 10$. Questa uguaglianza ci dice che (-25,65) (x=-25, y=65) è soluzione di $88x+34y=10$!!

Abbiamo risposto al seguente

PROBLEMA 2. Nel caso in cui ax+by=c abbia soluzioni intere trovare una soluzione.

RISPOSTA. Troviamo prima una soluzione di ax+by=d, d= M.C.D. (a,b), (ad esempio) con l'algoritmo di Euclide e poi la moltiplichiamo per c/d.

PROBLEMA 3. Nel caso in cui ax+by=c abbia soluzioni determinarle tutte.

RISPOSTA. Sommiamo ad una sua soluzione tutte le soluzioni dell'*equazione omogenea associata*.
(per la dim. cfr. dispense G.Niesi)

Lo terminiamo la prossima volta.

m