

Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2003/2004
ALGEBRA 1
Prof. M. Fontana
Tutorato 3 - Andrea Cova (17 ottobre 2003)

1. Siano $a, b \in \mathbb{Z}$, non entrambi nulli, allora il **minimo comune multiplo** di a e b (in breve, $\text{mcm}(a, b)$) è quell'intero $h \in \mathbb{N}$ tale che: 1) $a \mid h$ e $b \mid h$; 2) $h' \in \mathbb{Z}$ e $a \mid h', b \mid h' \Rightarrow h \mid h'$.
(L'ipotesi che $(a, b) \neq (0, 0)$, in questo caso, è un'ipotesi di comodo, per studiare le relazioni tra mcm e MCD ; infatti si può porre per definizione senza difficoltà:
 $\text{mcm}(0,0) := \text{mcm}(a,0) := \text{mcm}(0,b) := 0$.)
Poniamo $a\mathbb{Z} := \{ak : k \in \mathbb{Z}\}$. Mostrare che:
- (a) $a\mathbb{Z} \subset b\mathbb{Z} \Leftrightarrow b \mid a$;
 - (b) sia $h := \text{mcm}(a, b)$, allora: $h\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$;
 - (c) $\text{mcm}(ac, bc) = |c| \text{mcm}(a, b)$;
 - (d) $\text{MCD}(a, b) = 1 \Rightarrow \text{mcm}(a, b) = |ab|$;
 - (e) $\text{MCD}(a, b) \text{mcm}(a, b) = |ab|$;
 - (f) $\text{mcm}(a, b) = |b| \Leftrightarrow a \mid b \Leftrightarrow \text{MCD}(a, b) = |a|$;
 - (g) Sia $d := \text{MCD}(a, b)$, allora $a\mathbb{Z} \cup b\mathbb{Z} \subset d\mathbb{Z}$, ed inoltre: $a\mathbb{Z} \cup b\mathbb{Z} = d\mathbb{Z} \Leftrightarrow a \mid b$ oppure $b \mid a$.
2. Sia b un intero naturale $b \geq 2$. Mostrare che ogni $a \in \mathbb{N}^+$ si può scrivere in modo unico:
 $a = a_m b^m + a_{m-1} b^{m-1} + \dots + a_1 b + a_0$ con $a_m \neq 0$ e $0 \leq a_i \leq b - 1$ per ogni $0 \leq i \leq m$.
L'espressione precedente può essere abbreviata nella forma: $a = (a_m a_{m-1} \dots a_1 a_0)_b$;
tale scrittura prende il nome di **scrittura in base b di a** . Se $b = 10$, abbiamo l'usuale scrittura decimale dei numeri naturali.
3. Scrivere: (a) 1232 in base 5; (b) 10 in base 2; (c) 12 in base 12; (d) 1704 in base 12;
(e) 2145 in base 7; (f) 101 in base 2.
per la base 12, utilizzare i simboli 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, u, v.
4. Scrivere il MCD delle seguenti coppie di interi sotto forma di una identità di Bézout:
(a) (180, 252); (b) (-722, -415); (c) (625, 32); (d) (-5, 5).
5. (a) Sia $d = ax + by$ il $\text{MCD}(a, b)$. Mostrare con un esempio che tale espressione (Identità di Bézout) *non* è unica, cioè possono esistere altri due elementi $x', y' \in \mathbb{Z}$ con
 $d = ax + by = ax' + by'$.
- (b) Sia $ax_0 + by_0 = 1$. Preso comunque $n \in \mathbb{Z}$, se $x := x_0 + nb$ ed $y := y_0 - na$, allora mostrare che $ax + by = 1$.
- (c) Mostrare che se $ax_0 + by_0 = ax_1 + by_1 = 1$, allora esiste un intero n tale che $x_1 = x_0 + nb$ e $y_1 = y_0 - na$.
- (d) Mostrare che se $ax_0 + by_0 = ax_1 + by_1 = d$, allora esiste un intero n tale che $x_1 = x_0 + n \cdot \text{mcm}(a, b) / a$ e $y_1 = y_0 - n \cdot \text{mcm}(a, b) / b$.
6. Siano $a, b \in \mathbb{Z} \setminus \{0, 1, -1\}$ due interi di cui sia nota la fattorizzazione in primi:
 $a = \pm p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ $b = \pm p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$
con $e_i, f_i \geq 0$, $1 \leq i \leq r$ (in tale situazione, si può supporre che i fattori primi di a e b siano gli stessi!).
Mostrare che: $\text{MCD}(a, b) = p_1^{g_1} p_2^{g_2} \dots p_r^{g_r}$ con $g_i := \min(e_i, f_i)$, $1 \leq i \leq r$,
 $\text{mcm}(a, b) = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$ con $h_i := \max(e_i, f_i)$, $1 \leq i \leq r$.