Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2002/2003

ALGEBRA 1
Prof. M. Fontana
Tutorato 1- Andrea Cova (16 ottobre 2002)

1. Siano $a, b \in Z$, non entrambi nulli, allora il **minimo comune multiplo** di a e b (in breve, mcm (a, b)) è quell'interno $h \in N$ tale che: 1. $a \mid h$ e $b \mid h$; 2. $h' \in Z$ 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 (a, b) e MCD; infatti si può porre per definizione senza difficoltà:
   mcm(0, 0) := mcm(a, 0) := mcm(0, b) :=0.)
   Poniamo $x\,Z := \{ x\,k : k \in Z \}$. Mostrare che:
   (a) $a\,Z \subset b\,Z \Leftrightarrow b \mid a$;
   (b) sia h := mcm (a, b), allora: $h\,Z = a\,Z \cap b\,Z$;
   (c) mcm (ac, bc) = |c| mcm (a, b);
   (d) MCD (a, b) = 1 $\Rightarrow$ mcm (a, b) = |ab|;
   (e) MCD (a, b) mcm (a, b) = |ab|;
   (f) Mcm (a, b) = |b| $\Leftrightarrow a \mid b \Leftrightarrow$ MCD (a, b) = |a|;
   (g) Sia d := MCD (a, b), allora $a\,Z \cup b\,Z \subset d\,Z$, ed inoltre: $a\,Z \cup b\,Z = d\,Z \Leftrightarrow a \mid b$ oppure $b \mid a$.

2. Sia b un intero naturale $b \leq 2$. Mostrare che *ogni* $a \in N^+$ *si può scrivere in modo unico:*
   $a = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_1 b + a_0$ *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: $a = (a_m a_{m-1} \ldots a_1 a_0)_b$;
   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 MCD (a, b). Mostrare con un esempio che tale espressione (Identità di Bézout) *non* è unica, cioè possono esistere altri due elementi $x^1, y^1 \in Z$ con
   $$d = ax + by = ax' + by'.$$
   (b) Sia $ax_0 + by_0 = 1$. Preso comunque $n \in Z$, 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 esite un intero n tale che $x_1 = x_0 + n \bullet$ mcm (a, b) / a e y1 = y0 – n • mcm (a, b) / b.

6. Siano $a, b \in Z \setminus \{0, 1, -1\}$ due interi di cui sia nota la fattorizzazione in primi:
   $a = \pm p_1^{e1} p_2^{e2} \ldots p_r^{er}$ $\quad b = \pm p_1^{f1} p_2^{f2} \ldots p_r^{fr}$
   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: MCD (a, b) $= p_1^{g1} p_2^{g2} \ldots p_r^{gr}$ con $g_i := \min(e_i, f_i)$, $1 \leq i \leq r$,
   mcm (a, b) $= p_1^{h1} p_2^{h2} \ldots p_r^{hr}$ con $h_i := \max(e_i, f_i)$, $1 \leq i \leq r$.

7. Sia $n \in N^+$. Se $n \geq 2$ non è primo, allora, mostrare che esiste un primo p che divide n tale che $p \leq \sqrt{n}$.

Su tale proprietà è basato il **Crivello di Eratostene** (III sec. A.C.), semplice metodo algoritmico per determinare tutti i numeri primi $\leq \sqrt{n}$: *Si scrivano in una tabella tutti i numeri naturali tra* 2 *ed* n *e si cancellino tutti quelli tra questi che sono multipli propri dei numeri primi noti tra* 2 *e* $\sqrt{n}$. *I numeri restanti sono tutti e soli i numeri primi* $\leq$ n. A titolo d'esempio determinare, usando questo metodo, tutti i numeri primi minori di 100.