ALGEBRA 1 PB-Z
IV. 30 III 2012

Esercizio 1. Si calcoli il massimo comun divisore di $(903, -1784)$ e lo si scriva nella forma "identità di Bezout" .

Soluzione. Risulta $\mathrm{MCD}(903, -1784) = \{\pm 1\}$. Mostriamo questo risultando utilizzando l'algoritmo "euclideo delle divisioni successive". Innanzi tutto osserviamo che, da $1784 = 1 \cdot 903 + 881$, sottraendo e aggiungendo 903, otteniamo $-1784 = -1 \cdot 903 - 903 + 903 - 881 = -(1+1) \cdot 903 + (903 - 881)$; ossia,

$$-1784 = -2 \cdot 903 + 22, \quad 0 \leq 22 < |903|.$$

Proseguiamo poi con l'algoritmo:

$$\begin{array}{rcl} -1784 & = & -2 \cdot 903 + 22; \\ 903 & = & 41 \cdot 22 + \mathbf{1}; \\ 22 & = & 22 \cdot \mathbf{1} + 0; \end{array}$$

d'onde $\mathrm{MCD}(903, -1784) = \{\pm 1\}$, essendo 1 l'ultimo resto non nullo delle divisioni dell'algoritmo euclideo e ricordando che, in tutta generalità,

$$d \in \mathrm{MCD}(a, b) \;\Leftrightarrow\; -d \in \mathrm{MCD}(a, b),$$

per ogni $a, b \in \mathbb{Z}$.

Ora, "percorrendo a ritroso" l'algoritmo euclideo delle divisioni successive, è possibile scrivere $1 = (-41) \cdot (-1784) + (-81) \cdot 903$, essendo

$$\begin{array}{rcl} 1 & = & 903 - 41 \cdot 22 \; = \\ & = & 903 - 41 \cdot ((-1784) - (-2) \cdot 903) \; = \\ & = & (-41) \cdot (-1784) + (1 - 41 \cdot 2) \cdot 903 \; = \\ & = & (-41) \cdot (-1784) + (-81) \cdot 903. \end{array}$$

Esercizio 2. Siano gli interi $a_1, a_2, b \in \mathbb{Z}$ tali che $\mathrm{MCD}(a_1, b) = \{\pm 1\}$ e $\mathrm{MCD}(a_2, b) = \{\pm 1\}$. Si provi che, allora, $\mathrm{MCD}(a_1 a_2, b) = \{\pm 1\}$.

Sugg. Si prendano (x_1, y_1), $(x_2, y_2) \in \mathbb{Z}^2$ tali che $1 = x_1 a_1 + y_1 b$ e $1 = x_2 a_2 + y_2 b$, si trovi $(x, y) \in \mathbb{Z}^2$ tale che $1 = x a_1 a_2 + y b$ e si concluda.

Soluzione. *Metodo primo, usando le identità di Bezout.* **I.** Ricordo che, dati comunque interi $z', z'' \in \mathbb{Z}$, l'insieme $\mathrm{MCD}(z', z'')$ è l'insieme di tutti e soli i divisori w di z' e z'' della forma $w = h'z' + h''z''$, con $h', h'' \in \mathbb{Z}$. **II.** Torno all'esercizio e considero $z' = a_1a_2$ e $z'' = b$. **III.** Osservo che $1|a_1a_2$ e $1|b$. **IV.** Mi accorgo che, grazie al punto I., se trovassi interi $x, y \in \mathbb{Z}$ tali che $1 = xa_1a_2 + yb$, avrei concluso l'esercizio. **V.** Trovo $x, y \in \mathbb{Z}$ tali che $1 = xa_1a_2 + yb$ in questa maniera: **V.a.** Per ipotesi (e tenendo presente il punto I.), esistono (x_1, y_1), $(x_2, y_2) \in \mathbb{Z}^2$ tali che $1 = x_1a_1 + y_1b$ e $1 = x_2a_2 + y_2b$. **V.b.** Scrivo $1 = 1 \cdot 1$. **V.c.** Calcolo:

$$\begin{array}{rcl} 1 = 1 \cdot 1 & = & (x_1a_1 + y_1b) \cdot (x_2a_2 + y_2b) \; = \\ & = & (x_1x_2)a_1a_2 + ((x_1a_1)y_2 + (x_2a_2)y_1)b + (y_1y_2)b \; = \\ & = & (x_1x_2)a_1a_2 + ((1 - y_1b)y_2 + (1 - y_2b)y_1)b + (y_1y_2)b \; = \\ & = & (x_1x_2)a_1a_2 + ((1 - y_1b)y_2 + (1 - y_2b)y_1 + (y_1y_2))b \; = \\ & = & (x_1x_2)a_1a_2 + (y_1 + y_2 - 2y_1y_2b + y_1y_2)b \end{array}$$

V.d. Prendo $x = x_1x_2$ e $y = y_1 + y_2 - 2y_1y_2b + y_1y_2$.

Metodo secondo, usando il teorema di fattorizzazione unica. Siano $A_1 \subset \mathbb{Z}$, $A_2 \subset \mathbb{Z}$, $A \subset \mathbb{Z}$ e $B \subset \mathbb{Z}$ gli insiemi dei primi che appaiono nella fattorizzazione di a_1, a_2, a_1a_2 e, rispettivamente, b. **I.** Le ipotesi $\mathrm{MCD}(a_1, b) = \{\pm 1\}$ e $\mathrm{MCD}(a_2, b) = \{\pm 1\}$ implicano che $A_1 \cap B = \emptyset$ e, rispettivamente, $A_2 \cap B = \emptyset$. **II.** Osserviamo che $A = A_1 \cup A_2$. **III.** Deduciamo che $A \cap B = \emptyset$, essendo $A \cap B = (A_1 \cup A_2) \cap B = (A_1 \cap B) \cup (A_2 \cap B) = \emptyset$. **IV.** Concludiamo, osservando che, allora, $\mathrm{MCD}(a_1a_2, b) = \{\pm 1\}$, non avendo a_1a_2 e b fattori primi comuni.

Esercizio 3. Siano $a, b, c \in \mathbb{Z}$. Si dimostri che l'equazione $\triangle : aX + bY = c$ ammette soluzioni intere $(x, y) \in \mathbb{Z}^2$ se e solo se per ogni $d \in \mathrm{MCD}(a, b)$ vale $d|c$.

Sugg. ($\Rightarrow$) Se (x, y) è una soluzione di $\triangle$, allora ogni $d \in \mathrm{MCD}(a, b)$ divide c, perché... ($\Leftarrow$) Se $d \in \mathrm{MCD}(a, b)$, allora esistono $h, k \in \mathbb{Z}$ tali che... ...inoltre, poiché $d|c$, allora esiste...

Soluzione. ($\Rightarrow$) Sia d in $\mathrm{MCD}(a, b)$ un qualsiasi massimo comun divisore di a e b. Allora d divide ogni combinazione lineare a coefficienti interi di a e b, perché divide sia a che b. Quindi, in particolare, se (x, y) è una soluzione di $\triangle$, cioè se vale $ax + by = c$, allora d divide $c = ax + by$.

($\Leftarrow$) Sia d in $\mathrm{MCD}(a, b)$ un massimo comun divisore di a e b e siano $h, k \in \mathbb{Z}$ tali che $d = ha + kb$. Poiché (per ipotesi) $d|c$, esiste $q \in \mathbb{Z}$ tale che $c = qd$. Quindi,

$$\begin{array}{rcl} c & = & qd \; = \\ & = & q(ha + kb) \; = \\ & = & (qh)a + (qk)b \end{array}$$

e la coppia $(x, y) = (qh, qk) \in \mathbb{Z}^2$ è una soluzione intera di $\triangle$.

Esercizio 4. Si mostri che tutti e soli i sottogruppi ([1]) di $(\mathbb{Z}, +)$ sono della forma $n\mathbb{Z} = \{z \in \mathbb{Z} \text{ tale che } n|z\}$, con $n \in \mathbb{Z}$.

Sugg. Da un lato, per ogni $n \in \mathbb{Z}$, il sottoinsieme $n\mathbb{Z}$ è un sottogruppo di $\mathbb{Z}$ (lo si mostri!). Da un altro lato, se $(S, +) \leq (\mathbb{Z}, +)$ è banale, si può concludere osservando che... Se invece $(S, +) \leq (\mathbb{Z}, +)$ è non banale, allora si proceda come segue. Poiché S contiene elementi positivi (lo si mostri!), esiste $n \in S$ il minimo di tali elementi. Allora risulterà che $S = n\mathbb{Z}$; perché, da una parte, $S \supseteq n\mathbb{Z}$ (...immediato? lo si mostri!) e, da un'altra parte, $S \subseteq n\mathbb{Z}$, ogni elemento $s \in S$ appartenendo a $n\mathbb{Z}$ (si mostri quest'ultimo fatto come segue: dividendo s per n, si scriva $s = qn + r$, con $0 \leq r < n$, e si osservi che, allora, r è in S; infine, si usi la minimalità di $n \in S \cap \mathbb{Z}_{>0}$).

Soluzione. *Lato primo.* Per ogni $n \in \mathbb{Z}$, il sottoinsieme $n\mathbb{Z} \subseteq \mathbb{Z}$ è un sottogruppo di $(\mathbb{Z}, +)$. Infatti; **I.** il codominio di $+|_{n\mathbb{Z}\times n\mathbb{Z}}$ è contenuto in $n\mathbb{Z}$; ossia, $+|_{n\mathbb{Z}\times n\mathbb{Z}} : n\mathbb{Z} \times n\mathbb{Z} \to n\mathbb{Z}$, perché la somma di due multipli di n è anch'essa un multiplo di n (infatti $q_1 n + q_2 n = (q_1 + q_2)n$). **II.** Il sottoinsieme $n\mathbb{Z} \subseteq \mathbb{Z}$ contiene 0 (infatti $0 = 0n$). **III.** Se a è in $n\mathbb{Z}$, allora $-a$ è pure in $n\mathbb{Z}$ (infatti se $a = qn$, allora $-a = (-q)n$).

Lato secondo. Se $(S, +)$ un sottogruppo banale di $(\mathbb{Z}, +)$, allora o $S = \mathbb{Z}$ oppure $S = \{0\}$. Nel primo caso $S = 1\mathbb{Z}$, nel secondo caso $S = 0\mathbb{Z}$. Sia, dunque, $(S, +)$ un sottogruppo non banale di $(\mathbb{Z}, +)$. Allora in S esistono elementi positivi; ossia $S \cap \mathbb{Z}_{>0} \neq \emptyset$. Infatti, essendo non banale, in particolare abbiamo che $S \neq \{0\}$. Dunque, in S esiste almeno un elemento non nullo s. Ora, **essendo un gruppo**, oltre a contenere s, $(S, +)$ contiene anche $-s$. Poiché uno tra s e $-s$ è senz'altro positivo, abbiamo che $S \cap \mathbb{Z}_{>0} \neq \emptyset$. Sia n l'elemento minimo di $S \cap \mathbb{Z}_{>0} \subseteq \mathbb{N}$; cioè sia $n = \min\{S \cap \mathbb{Z}_{>0}\}$. Allora $S = n\mathbb{Z}$. Infatti, da una parte $S \supseteq n\mathbb{Z}$, perché S, essendo un gruppo, contiene tutti i multipli di ogni suo elemento (così che, in particolare, contiene tutti i multipli di n; ossia, tutto $n\mathbb{Z}$). Da un'altra parte, mostriamo che $S \subseteq n\mathbb{Z}$, provando che ogni $s \in S$ è contenuto in $n\mathbb{Z}$. La dimostrazione di questo fatto è basata sulla seguente osservazione. Si prenda $s \in S$ e lo si divida per n, cioè, si scriva $s = qn + r$, con $0 \leq r < n$, e si proceda osservando che, allora, r appartiene a S, in quanto differenza di due elementi di S. Infatti, $r = s - qn = s + (-q)n$, con $s \in S$ e $(-q)n \in n\mathbb{Z} \subseteq S$. Dunque, ricapitolando, r è in S, perché differenza di due elementi di S (si osservi che, nel dedurre quest'ultimo fatto, si usa tutta la forza dell'ipotesi: $(S, +) < (\mathbb{Z}, +)$ è un sottogruppo di $\mathbb{Z}$). Ora, l'intero r, essendo un elemento di S che **1.** è non negativo e **2.** è strettamente minore di n, deve essere necessariamente uguale a 0, 'ché, altrimenti, r sarebbe strettamente positivo e, in quanto tale, apparterrebbe a $S \cap \mathbb{Z}_{>0}$; in tal caso, però arriveremmo a una contraddizione, perché, allora $r \in S$ sarebbe contemporaneamente e strettamente minore di n (per 2.) e maggiore o uguale a n (perché $n = \min\{S \cap \mathbb{Z}_{>0}\}$). Dunque $r = 0$. Così abbiamo $s = qn + r = qn + 0$; cioè, $s = qn$; ossia, s è in $n\mathbb{Z}$. Per la genericità di s in S, abbiamo dunque $S \subseteq n\mathbb{Z}$.

[1] Sia $(G, \bigstar)$ un gruppo. Un sottoinsieme non vuoto H di G è un **sottogruppo di** $(G, \bigstar)$ sse la restrizione di $\bigstar$ a $H \times H$ definisce su H una struttura di gruppo; ossia, sse $(H, \bigstar|_{H\times H})$ è un gruppo. La notazione abituale per H sottoinsieme di G che sia anche un sottogruppo è $H \leq G$.

Esercizio 5. Si fissi un intero $m \in \mathbb{Z}$, $m \geq 2$. Siano $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ interi per i quali esistono $q', q'' \in \mathbb{Z}$ tali che $a_1 = a_2 + q'm$ e $b_1 = b_2 + q''m$. Si dimostri che, allora, esistono $\hat{q},\ \tilde{q} \in \mathbb{Z}$ tali che $(a_1 + b_1) = (a_2 + b_2) + \hat{q}m$ e $(a_1 b_1) = (a_2 b_2) + \tilde{q}m$.

Oss. Svolgendo l'esercizio, avete mostrato che, se $a_1 \equiv_m a_2$ e $b_1 \equiv_m b_2$, allora $a_1 + b_1 \equiv_m a_2 + b_2$ e $a_1 b_1 \equiv_m a_2 b_2$. Per cui, svolgendo l'esercizio, avete dimostrato che le seguenti definizioni di addizione e moltiplicazione su $\mathbb{Z}/\equiv_m$ sono ben poste: $[a] + [b] := [a + b]$ e $[a] \cdot [b] := [ab]$ ([2]).

Soluzione. Più. Da $a_1 = a_2 + q'm$ e $b_1 = b_2 + q''m$, abbiamo $a_1 + b_1 = (a_2 + q'm) + (b_2 + q''m)$; ossia,

$$a_1 + b_1 = a_2 + b_2 + (q' + q'')m.$$

Per cui, l'intero $\hat{q} = q' + q''$ fa al caso nostro.

Per. Da $a_1 = a_2 + q'm$ e $b_1 = b_2 + q''m$, abbiamo $a_1 b_1 = (a_2 + q'm) \cdot (b_2 + q''m)$; ossia,

$$a_1 b_1 = a_2 b_2 + (q' b_2 + q'' a_2)m + q' q'' m^2;$$

ossia,

$$a_1 b_1 = a_2 b_2 + (q' b_2 + q'' a_2 + q' q'' m)m.$$

Per cui, l'intero $\tilde{q} = q' b_2 + q'' a_2 + q' q'' m$ fa al caso nostro.

[2]Sulla buona posizione delle operazioni $+$ e $\cdot$ su $\mathbb{Z}/\equiv_m$. **1.** Per ogni $A, B \in \mathbb{Z}/\equiv_m$, si scelgono rappresentanti $a \in A$ e $b \in B$ (da cui $A = [a]$ e $B = [b]$) e **2.** si definiscono la classe $\mathrm{S}_{A,B} \in \mathbb{Z}/\equiv_m$, somma di A e B, e la classe $\mathrm{P}_{A,B} \in \mathbb{Z}/\equiv_m$, prodotto di A e B, ponendo $\mathrm{S}_{A,B} = [a + b]$ e $\mathrm{P}_{A,B} = [ab]$. **3.** Si osserva che le classi $\mathrm{S}_{A,B}$ e $\mathrm{P}_{A,B}$ sono definite per mezzo di alcuni loro rappresentanti specifici: nel nostro caso essi sono $a + b$ e, rispettivamente, ab; quindi, in ultima istanza le classi $\mathrm{S}_{A,B}$ e $\mathrm{P}_{A,B}$ dipendono dai rappresentanti a di A e b di B scelti in 2. **4.** Si mostra che, di fatto, esse non dipendono dalla scelta di tali rappresentanti. Svolgendo l'esercizio, avete mostrato il punto 4. della presente nota.