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" .

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.

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 $d \in \mathrm{MCD}(a, b)$ 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...

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 $n \in S \cap \mathbb{Z}_{>0}$).

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]).

---

[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 $H \leq G$.

[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.