ESERCIZI SU

M.C.D. E EQUAZIONI DIOFANTEE

N.B.: il simbolo ☡ contrassegna gli esercizi (relativamente) più complessi.

— ∗ —

1 — Sia "$\big|$" la relazione di divisibilità in $\mathbb{Z}$. Siano $a, e \in \mathbb{Z}$ tali che $\mathrm{MCD}(a,e) = 1$. Dimostrare che, per ogni $z \in \mathbb{Z}$, se $a\big|z$ e $e\big|z$ allora anche $(a\,e)\big|z$.

2 — Sia "$\big|$" la relazione di divisibilità in $\mathbb{Z}$. Siano $a, b, d, h, k \in \mathbb{Z}$ tali che $d\,\big|a$, $d\,\big|b$ e $d = a\,h + b\,k$. Dimostrare che allora $d = \mathrm{MCD}(a,b)$.

3 — *(a)* Per ogni $a, b, t \in \mathbb{Z}$, dimostrare che $\mathrm{MCD}\big(a\,t, b\,t\big) = \mathrm{MCD}(a,b)\,t$.

(b) Per ogni $a, b \in \mathbb{Z}$, sia $d := \mathrm{MCD}(a,b)$. Dimostrare che $\mathrm{MCD}\big(a/d\,,\, b/d\,\big) = 1$.

<u>*Suggerimento:*</u> *Per dimostrare la parte (b), si utilizzi il risultato in (a) e il fatto che il prodotto in $\mathbb{Z}$ sia cancellativo.*

4 — Sia "$\big|$" la relazione di divisibilità in $\mathbb{Z}$, sia $\equiv_n$ la relazione di congruenza modulo $n \in \mathbb{N}_+$, e siano $d, z', z'' \in \mathbb{Z}$ tali che $d\,\big|n$ e $z' \equiv_n z''$.

(a) Dimostrare che $d\,\big|z' \iff d\,\big|z''$.

(b) Dimostrare che $\mathrm{MCD}\big(z', n\big) = \mathrm{MCD}(z'', n)$.

<u>*Suggerimento:*</u> *La parte (b) è conseguenza diretta del risultato in (a).*

5 — Sia "$\big|$" la relazione di divisibilità in $\mathbb{Z}$, e siano $a, b, d \in \mathbb{Z}$ tali che $d\,\big|(ab)$ e $\mathrm{MCD}(a, d\,) = 1$. Dimostrare che allora $d\,\big|b$.

6 — Per ogni $a, b, c \in \mathbb{Z}$, dimostrare che

$$\mathrm{MCD}(a\,b\,, c\,) = 1 \quad \iff \quad \big(\mathrm{MCD}(a\,, c\,) = 1\big)\ \&\ \big(\mathrm{MCD}(b\,, c\,) = 1\big)$$

<u>*Suggerimento:*</u> *Per dimostrare l'implicazione "$\Leftarrow$" si utilizzi l'esercizio* **5** *qui sopra.*

7 — Calcolare $\mathrm{MCD}(a,b)$ per ciascuna delle seguenti coppie (a,b) di numeri interi: $(a,b) := (4567, -668)$, $(a,b) := (-4567, 668)$ e $(a,b) := (-4567, -668)$.

8 — Calcolare un $\mathrm{MCD}(a,b)$ ed una identità di Bézout corrispondente per i seguenti valori di a e b :

(I) $a=-237$, $b=81$; *(II)* $a=616$, $b=427$; *(III)* $a=1137$, $b=-419$.

<u>Soluzione</u>: *(I)* $\mathrm{MCD}(-237,81) \;=\; 3 \;=\; (-237)\cdot(-13)+81\cdot(-38)$

(II) $\mathrm{MCD}(616,427) \;=\; 7 \;=\; 616\cdot(-9)+427\cdot 13$

(III) $\mathrm{MCD}(1137,-419) \;=\; 1 \;=\; 1137\cdot 206+(-419)\cdot 559$

9 — Calcolare $\mathrm{MCD}(726,275)$ ed una identità di Bézout per esso.

10 — *(a)* Calcolare $\mathrm{MCD}(1812,724)$ ed una identità di Bézout per esso.

(b) Calcolare, se possibile, una soluzione per ciascuna delle due equazioni diofantee

$$1812\,x+724\,y \;=\; 14 \quad , \qquad 1812\,x+724\,y \;=\; 12 \quad .$$

11 — Dimostrare la seguente variante del teorema di esistenza della "divisione euclidea" tra numeri interi:

(a) Per ogni $a,b\in\mathbb{Z}$, con $b\neq 0$, esistono $q,r\in\mathbb{Z}$ tali che

$$a \;=\; b\,q+r \qquad \& \qquad 0\leq |r| \lneqq |b|$$

(b) Dimostrare inoltre che, in generale, tali q ed r *non* sono unici.

(c) Determinare per quali coppie $(a,b)\in\mathbb{Z}\times\mathbb{Z}$ la coppia (q,r) di "quoziente" e "resto" nella "divisione di a per b" al punto *(a)* sia univocamente determinata.

12 — Siano $\circledast' : a'x+b'y \;=\; c'$ e $\circledast'' : a''x+b''y \;=\; c''$ due equazioni diofantee. Dimostrare che se esiste $q\in\mathbb{Z}$ tale che $a''=q\,a'$, $b''=q\,b'$, $c''=q\,c'$, allora le due equazioni sono equivalenti, cioè hanno lo stesso insieme di soluzioni.

<u>Suggerimento</u>: *Si utilizzi il fatto che il prodotto in $\mathbb{Z}$ è cancellativo.*

13 — Calcolare, se esiste, una soluzione $\big(x',y'\big)\in\mathbb{Z}^2:=\mathbb{Z}\times\mathbb{Z}$ per ciascuna delle seguenti equazioni diofantee:

(a) $31\,x+12\,y \;=\; -5$; *(b)* $34\,x+(-51)\,y \;=\; 14$;

(c) $34\,x+(-51)\,y \;=\; 17$; *(d)* $389\,x+(-167)\,y \;=\; 5$;

<u>Soluzione</u>: *(a)* $\big(x',y'\big) \;=\; \big(25,-65\big)$; *(b)* <u>non esistono</u> soluzioni;

(c) $\big(x',y'\big) \;=\; \big(2,1\big)$; *(d)* $\big(x',y'\big) \;=\; \big(410,955\big)$.

14 — *(a)* Calcolare $\mathrm{MCD}(267,112)$ ed una identità di Bézout per esso.

(b) Calcolare, se possibile, una soluzione dell'equazione diofantea $267\,x+112\,y \;=\; 14$.

15 — *(a)* Calcolare M.C.D.$(132\,, -990)$.

(b) Determinare una identità di Bézout per M.C.D.$(132\,, -990)$.

(c) Calcolare, se possibile, una soluzione per ciascuna delle due equazioni diofantee seguenti:
$$(c.1)\quad -990\,x + 132\,y \;=\; 196 \quad , \qquad (c.2)\quad -990\,x + 132\,y \;=\; -198$$

16 — Determinare se esista almeno una soluzione per ciascuna delle seguenti equazioni diofantee:
$$(a)\quad 252\,x + 117\,y \;=\; 28 \quad , \qquad (b)\quad 117\,x + (-252)\,y \;=\; 36$$

In caso negativo, si spieghi perché non esistano soluzioni; in caso positivo, si calcoli esplicitamente una soluzione particolare.

17 — Si consideri l'equazione diofantea *omogenea*
$$\circledast_0 \;:\; a\,x + b\,y \;=\; 0 \qquad \big(\,a, b \in \mathbb{Z}\,\big)$$
e sia $\mathcal{S}_0 := \big\{\,(x_0, y_0) \in \mathbb{Z}^2 \,\big|\, (x_0, y_0) \text{ è soluzione di } \circledast_0 \big\}$ l'insieme delle sue soluzioni.

(a) Nel caso $(a, b) = (0, 0)$, dimostrare che $\mathcal{S}_0 \;=\; \mathbb{Z}^2$.

(b) Nel caso $(a, b) \neq (0, 0)$, dimostrare che $\mathcal{S}_0 \;=\; \big\{(\,b'z\,, -a'z) \,\big|\, z \in \mathbb{Z}\,\big\}$ dove
$$a' \;:=\; a \Big/ \mathrm{MCD}(a, b) \qquad \text{e} \qquad b' \;:=\; b \Big/ \mathrm{MCD}(a, b)\,.$$

18 — Dati $a, b, c \in \mathbb{Z}$, si considerino le due equazioni diofantee
$$\circledast \;:\; a\,x + b\,y \;=\; c \quad , \qquad \circledast_0 \;:\; a\,x + b\,y \;=\; 0$$
di cui la seconda si dice "equazione diofantea omogenea associata" alla prima, e si denotino con $\mathcal{S}$ e $\mathcal{S}_0$ rispettivamente l'insieme di tutte le soluzioni dell'equazione $\circledast$ e $\circledast_0$.

Dimostrare che
$$\mathcal{S} \;=\; \big(x', y'\big) + \mathcal{S}_0 \;=\; \big\{\big(x', y'\big) + (x_0, y_0) \,\big|\, (x_0, y_0) \in \mathcal{S}_0\,\big\}$$
dove $\big(x', y'\big) \in \mathcal{S}$ è una qualunque soluzione di $\circledast$.

19 — Calcolare *tutte* le soluzioni intere (se esistono) dell'equazione diofantea
$$-256\,x + 48\,y \;=\; 4$$

20 — Calcolare *tutte* le soluzioni intere (se esistono) dell'equazione diofantea
$$16\,x + 41\,y \;=\; -5$$

21 — Calcolare *tutte* le soluzioni intere (se esistono) dell'equazione diofantea
$$2000000007\,x + 1000000000\,y \;=\; 3$$

22 — Calcolare *tutte* le soluzioni intere (se esistono) dell'equazione diofantea

$$165\,x + 44\,y \;=\; 121$$

23 — Calcolare *tutte* le soluzioni intere (se esistono) delle due equazioni diofantee

$$34\,x + 51\,y \;=\; 171 \quad , \qquad 35\,x - 42\,y \;=\; 14$$

24 — Calcolare *tutte* le soluzioni intere (se esistono) delle equazioni diofantee

$$35\,x - 14\,y \;=\; 13 \quad , \qquad 6\,x + 21\,y \;=\; 51$$

25 — Determinare se esista una soluzione per ciascuna delle due equazioni diofantee seguenti: *(a)* : $27\,x \,+\, 18\,y \;=\; 48$, *(b)* : $27\,x \,+\, 18\,y \;=\; -45$

In caso positivo, calcolare esplicitamente una tale soluzione. In caso negativo, spiegare perché una tale soluzione non esista.

26 — Determinare se esista una soluzione per ciascuna delle due equazioni diofantee seguenti: *(a)* : $18\,x \,+\, 27\,y \;=\; 51$, *(b)* : $18\,x \,+\, 27\,y \;=\; -63$

In caso positivo, calcolare esplicitamente una tale soluzione. In caso negativo, spiegare perché una tale soluzione non esista.

27 — Per ogni $z \in \mathbb{Z}$, calcolare $\mathrm{MCD}(z{+}1, z)$ e $\mathrm{MCD}(z{+}2\,, z)$.

Suggerimento: *Nel secondo caso, si esaminino separatamente i casi z pari e z dispari.*

28 — È vero che ogni soluzione intera dell'equazione diofantea $20\,x + 10\,y \;=\; 0$ è anche soluzione dell'equazione $4\,x + 2\,y \;=\; 0$ e dell'equazione $2\,x + y \;=\; 0$? È vero il viceversa?

29 — È vero che ogni soluzione intera dell'equazione diofantea $20\,x + 10\,y \;=\; 10$ è anche soluzione dell'equazione $4\,x + 2\,y \;=\; 2$? È vero il viceversa?

30 — A partire dall'identità $623 \cdot 30 - 45 \cdot 413 \;=\; 105$, determinare quali possano essere — *senza calcolarli* esplicitamente — i valori di $\mathrm{MCD}(623, 413)$, di $\mathrm{MCD}(30, 413)$, di $\mathrm{MCD}(623, 45)$ e di $\mathrm{MCD}(30, 45)$.

31 — A partire dall'identità $62 \cdot 61728 - 97 \cdot 39455 \;=\; 1$, determinare (*senza calcolarli* esplicitamente) i valori di $\mathrm{MCD}(62, 97)$, di $\mathrm{MCD}(62, 39455)$, di $\mathrm{MCD}(61728, 39455)$ e di $\mathrm{MCD}(61728, 97)$.