Exercici 16. Siguin $a_1, a_2, ..., a_n \in \mathbb{Z}$ i $d = \text{mcd}(a_1, a_2, ..., a_n)$

(a) Demostreu que existeixen nombres enters $r_1, r_2, ..., r_n$ tals que $r_1a_1 + r_2a_2 + \cdots + r_na_n = d$.

(b) Calculeu nombres enters r, s, t tals que $17r + 51s + 45t = 1$ o be demostreu que no existeixen

Solucio 16 LEMA:$\text{mcd}(a_1, a_2, ..., a_n) = \text{mcd}(a_1, \text{mcd}(a_2, ..., a_n))$, ho provarem per induccio sobre n, $n = 3$: Tenim que sigui $\text{mcd}(a_1, a_2, a_3) = d$ i $\text{mcd}(a_2, a_3) = l$, sabem per Bezout que $\exists\ x, y \in \mathbb{Z}$ tals que $a_2x + a_3y = l$ i com $d|a_2$ i $d|a_3$, clarament $d|a_2x + a_3y = l$, ara veurem que $\nexists\ r > d$ tal que $r|a_1$ i $r|l$, suposem que existeix, aleshores tindriem que $r|l$ i $l|a_2$ i $l|a_3$ i per la transitivitat de $|$ tenim que $r|a_2$ i $r|a_3$ i com tambe hem suposat que $r|a_1$ i a mÃ©s $r > d$. tindriem que $\text{mcd}(a_1, a_2, a_3) >= r$, cosa totalment contardictoria, ara suposem que $\forall\ n > 3$ es compleix que $\text{mcd}(a_1, a_2, ..., a_n) = \text{mcd}(a_1, \text{mcd}(a_2, ..., a_n))$, demostrarem que per $n+1$, tambe; sigui $\text{mcd}(a_1, a_2, ..., a_{n+1}) = d$ i $\text{mcd}(a_2, ..., a_{n+1}) = l$, tenim que aplicant succesivament la Hipotesi d'induccio tenim que $\text{mcd}(a_2, \text{mcd}(a_3, ...\text{mcd}(a_n, a_{n+1}))) = l$, ara sabem que per l'dentitat de Bezout per certs $r_n, r_{n+1} \in \mathbb{Z}$ es te que $a_nr_n + a_{n+1}r_{n+1} = \text{mcd}(a_n, a_{n+1}) = k$ i per $\text{mcd}(a_{n-1}, k) = a_{n-1}r_{n-1} + ks = a_{n-1}r_{n-1} + a_nr_ns + a_{n+1}r_{n+1}s$, si anem repetint aquests pasos succesivament obtindrem per certs enters $a_2s_2 + \cdots + a_{n+1}s_{n+1} = l$. Ara toranant a la demostracio incial tenim que com $d|a_i\ \forall 1 \leq i \leq n+1$ i per tant $d|a_2s_2 + \cdots + a_{n+1}s_{n+1} = l$ provarem que $\nexists\ p > d$ tal que $p|l$ i $p|a_1$, supostem que existis, aleshores com $p|l$ i $l|a_i$ $\forall 2 \leq i \leq n+1$, tenim que $p|a_i\ \forall 2 \leq i \leq n+1$, pero llavors $\text{mcd}(a_1, a_2, ..., a_{n+1}) >= p$, cosa que es una contradiccio, i per tant tenim que $\nexists\ p > d$ tal que $p|l$ i $p|a_1 \implies \text{mcd}(a_1, a_2, ..., a_{n+1}) = d = \text{mcd}(a_1, \text{mcd}(a_2, ..., a_{n+1}))$.

i per tant hem provat que $\text{mcd}(a_1, a_2, ..., a_n) = \text{mcd}(a_1, \text{mcd}(a_2, ..., a_n))$

(a) Tenim que pel lema anterior $d = \text{mcd}(a_1, a_2, ..., a_n) = \text{mcd}(a_1, \text{mcd}(a_2, ..., a_n)) = \text{mcd}(a_1, \text{mcd}(a_2, \text{mcd}(a_3..., a_n))) = \text{mcd}(a_1, \text{mcd}(a_2, \text{mcd}(a_3, ...\text{mcd}(a_{n-1}, a_n))$, ara sabem que per la identitat de Bezout que $\exists s_{n-1}, s_n \in \mathbb{Z}$ tals que $\text{mcd}(a_{n-1}, a_n) = a_{n-1}s_{n-1} + a_ns_n$, ara tambÃ© tenim que per certs $s_{n-2}, is \in \mathbb{Z}$ es compleix que $\text{mcd}(a_{n-2}, \text{mcd}(a_{n-1}, a_n)) = a_{n-2}s_{n-2} + \text{mcd}(a_{n-1}, a_n)s = a_{n-2}s_{n-2} + a_{n-1}s_{n-1}s + a_ns_ns$, si anem repetint aquest proces succesivament tenim que haurem trobat $r_1, r_2, ..., r_n$ tals que

$$r_1a_1 + r_2a_2 + \cdots + r_na_n = d$$

. Que es el que voliem demostrar.

(b) Tenim que fet us del proces amb el qual hem demostrat la propietat de l'apartat anterior, podem calcular certs enters tals que $17r + 51s + 45t = 1$, tenim que aquests enters existeixen ja que $\text{mcd}(17, 51, 45) = 1$, ja que els dos unics divisors de 17, son 1 i ell mateix al ser primer. i com 17 no divideix 45, ens queda que l'unic divisors comu enter tots el nombres es 1. Ara tenim que $\text{mcd}(51, 45) = \text{mcd}(45, 6) = \text{mcd}(6, 3) = \text{mcd}(3, 0) = 3$, i revertint el calcul de l'algorsime d'Euclides, tenim que $3 = 45 - 6 \cdot 7 = 45 - (51 - 45) \cdot 7 = 45 \cdot 8 - 51 \cdot 7$, ara tenim que com $\text{mcd}(17, 3) = 1$, $\exists x, r \in \mathbb{Z}$ tals que $3x + 17r = 1$, podem notar que per $r = -1$ i $x = 6$, es compleix la igualtat, per tant per

$$r = -1, s = -42, t = 48,$$

es compleix la igualtat.