Manuel Ledo

# Exercise 2 Magistral classes

Given the extended euclids algorithm in matricial way $R_0 = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix}$ $Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$

$R_i = Q_i \cdot \ldots \cdot Q_1 \cdot R_0$, $0 \le i \le l$.

$s_0 = 1 \quad t_0 = 0$

$s_1 = 0 \quad t_1 = 1$

The following lemma holds

Lemma

i) $R_i \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$ iii) $\gcd(f,g) = \gcd(r_i, r_{i+1}) + 1$ v) $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$

ii) $R_i = \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix}$ iv) $s_i f + t_i g = r_i$ vi) $\gcd(r_i, t_i) = \gcd(f, t_i)$

In class we proved i), ii) and iii), so we are going to assume that both 3 properties hold in order to prove the rest. (the ones asked as an exercise).

iv) $s_i f + t_i g = r_i$: This equality follows directly from i) and ii)

$$\begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} \Rightarrow \begin{array}{l} s_i f + t_i g = r_i \\ s_{i+1} f + t_{i+1} g = r_{i+1} \end{array} \qquad \forall i \in \{0, \ldots l\}$$

v) $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$: This equality follows from ii)

Observe that $s_i t_{i+1} - t_i s_{i+1} = \det R_i = \det Q_i \cdots \det Q_1 \cdot \det R_0$

$\det Q_i = -1$ $\forall i$ and $\det R_0 = 1$, so $\det R_i = (-1)^i$. Thus,

$s_i t_{i+1} - t_i s_{i+1} = (-1)^i$ as we wanted to prove.

vi) $\gcd(r_i, t_i) = \gcd(f, t_i)$: One should note that v) in particular implies that $\gcd(s_i, t_i) = 1$. Suppose that $\exists p \in R$ such that $p \mid t_i$, if $p \mid f$ then $p \mid s_i f + t_i g = r_i$.

If $\exists p \in R$ such that $p \mid r_i$, then $p \mid s_i f = r_i - t_i g$ and $p \mid f$ since $\gcd(s_i, t_i) = 1$