

Trabalho extra II

Fernando Ferreira

Introdução à Teoria dos Números
2018/2019

Nesta sequência de exercícios mostramos que os números que ocorrem no algoritmo estendido de Euclides estão limitados adequadamente (ver a última alínea abaixo) e que, portanto, o algoritmo estendido também é eficiente.

Fixamos a e b números naturais com $a > b$ e $b \nmid a$. Ponha-se $r_0 = a$, $r_1 = b$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$ e $t_1 = 1$ e, recursivamente, $r_{i+1} = r_{i-1} - q_i r_i$, $s_{i+1} = s_{i-1} - q_i s_i$ e $t_{i+1} = t_{i-1} - q_i t_i$ até se atingir um passo k tal que $r_{k+1} = 0$ (aqui, q_i e r_{i+1} são, respectivamente, o cociente e o resto da divisão de r_{i-1} por r_i). Como sabemos, $\text{mdc}(a, b) = r_k$.

1. Mostre que $s_i s_{i+1} \leq 0$ e $t_i t_{i+1} \leq 0$, para todo i com $0 \leq i \leq k$. (Proceda indutivamente.)
2. Mostre que $|s_i| \leq |s_{i+1}|$ and $|t_i| \leq |t_{i+1}|$ para $1 \leq i \leq k$.
3. Mostre que $as_i + bt_i = r_i$, para todo i com $0 \leq i \leq k+1$. (Note, em particular, que $as_k + bt_k = \text{mdc}(a, b)$ e que $as_{k+1} + bt_{k+1} = 0$.)
4. Para cada i tal que $1 \leq i \leq k+1$ considere-se a matriz de 2×2 ,

$$A_i := \begin{bmatrix} s_{i-1} & s_i \\ t_{i-1} & t_i \end{bmatrix}$$

Mostre que, para todo i com $1 \leq i \leq k$, se tem

$$A_{i+1} = A_i \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix}$$

5. Mostre que, para todo i com $1 \leq i \leq k+1$, se tem $\det(A_i) = (-1)^{i-1}$.
6. Mostre que $s_{k+1} \neq 0$, $t_{k+1} \neq 0$ e que $|s_{k+1}| \perp |t_{k+1}|$. (Sugestão: para a coprimidade, ponha $i = k+1$ na alínea anterior.)
7. Mostre que $s_{k+1} \mid b$ e que $t_{k+1} \mid a$. Mostre também que $\left| \frac{b}{s_{k+1}} \right| = \left| \frac{a}{t_{k+1}} \right|$.
8. Seja d o valor comum da alínea anterior. Mostre que $d = \text{mdc}(a, b)$. Sugestão: calcule $\text{mdc}(|s_{k+1}|, |t_{k+1}|)$.
9. Mostre que $|s_i| \leq \frac{b}{\text{mdc}(a, b)}$ e $|t_i| \leq \frac{a}{\text{mdc}(a, b)}$ para $0 \leq i \leq k+1$. (Use as alíneas 2, 7 e 8.)