3.5 1) L'exercice 3.3 assure que $\mathrm{D}(a,b) = \mathrm{D}(b,r)$.

Ainsi le plus grand élément de $\mathrm{D}(a,b)$ est le même que le plus grand élément de $\mathrm{D}(b,r)$.

En d'autres termes, $\mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,r)$.

2) En appliquant la formule $\mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,r)$ à la suite des divisions euclidiennes de l'algorithme

$$\begin{array}{rrll}
a = & b \cdot q_1 & + \ r_1 & (r_1 \neq 0) \\
b = & r_1 \cdot q_2 & + \ r_2 & (r_2 \neq 0) \\
r_1 = & r_2 \cdot q_3 & + \ r_3 & (r_3 \neq 0) \\
 & \vdots & & \\
r_{n-2} = & r_{n-1} \cdot q_n & + \ r_n & (r_n \neq 0) \\
r_{n-1} = & r_n \cdot q_{n+1} & &
\end{array}$$

on obtient :

$\mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,r_1) = \mathrm{pgcd}(r_1,r_2) = \mathrm{pgcd}(r_2,r_3) = \ldots = \mathrm{pgcd}(r_{n-1},r_n)$

Il reste donc à prouver que $\mathrm{pgcd}(r_{n-1},r_n) = r_n$.

La dernière égalité $r_{n-1} = r_n \cdot q_{n+1}$ montre que r_n est un diviseur de r_{n-1}.

Comme r_n est le plus grand diviseur possible de r_n, on conclut que $\mathrm{pgcd}(r_{n-1},r_n) = r_n$.