

Please include a copy of this page as a cover sheet for your homework paper.

(See problem 3.28 of the text.) Let $a > b > 0$ be integers and let q_j, r_j be the quotients and remainders, respectively, obtained from the Euclidean algorithm applied to a and b :

$$\begin{aligned} a &= q_1b + r_1 \\ b &= q_2r_1 + r_2 \\ r_1 &= q_3r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k. \end{aligned}$$

- Let c be any common divisor of a and b . Show that c must divide r_1 ; use this to show that c also must divide r_2 .
- Let c be as in part a. Use induction to show that c must divide r_j for all j . In particular, this shows that c divides r_k , (the last non-zero remainder).
- Use induction to show that r_k divides r_j for $1 \leq j \leq k$.
- Use part c with $j = 1, 2$ to show that r_k divides each of a and b .
- Use part b to show that $r_k \geq c$ for any common divisor c of a and b and then use part d to show that $r_k = \gcd(a, b)$.
- Use the quotients q_j to define two sequences recursively:

$$\begin{aligned} x_0 &= 0, & x_1 &= 1, & x_j &= -q_{j-1}x_{j-1} + x_{j-2}, \\ y_0 &= 1, & y_1 &= 0, & y_j &= -q_{j-1}y_{j-1} + y_{j-2}. \end{aligned}$$

Use induction to show that for $1 \leq j \leq k$,

$$r_j = ay_{j+1} + bx_{j+1}.$$

Now use part e to conclude that the extended Euclidean algorithm produces the correct result, i.e., that $\gcd(a, b) = ay_{k+1} + bx_{k+1}$.