Euclid's algorithm

Recall:

- "m divides n" if $\frac{n}{m}$ is integer
- "c is a common divisor of a and b" if c divides a and c divides b
- $c = \gcd(a,b)$ if c is a common divisor, and is the largest number with this property
- When $\gcd(a,b) = 1$, we say "a and b are co-prime"

The algorithm: Given are two integers $a, b > 0$.

Initialize: $r_0 := a$
$r_1 := b$

Step $i \to i+1$: Define q_{i+1}, r_{i+1} as quotient and remainder of the Euclidean (i.e. integer) division $\frac{r_{i-1}}{r_i}$:

$$r_{i-1} = q_{i+1} r_i + r_{i+1}$$

Termination criterion: Terminate if $r_{i+1} = 0$, then $c = r_i$ is $\gcd(a,b)$.
Otherwise, iterate Step.

Example: $a = 10$, $b = 15$

$r_0 = 10$
$r_1 = 15$

$i=1$: $10 = q_2\, 15 + r_2$ $\Rightarrow$ $q_2 = 0$, $r_2 = 10$

$i=2$: $15 = q_3\, 10 + r_3$ $\Rightarrow$ $q_3 = 1$, $r_3 = 5$

$i=3$: $10 = q_4\, 5 + r_4$ $\Rightarrow$ $q_4 = 2$, $r_4 = 0$, Termination

$\Rightarrow \gcd(10, 15) = r_3 = 5$

Why does it work?

First, observe that r_i, $i \geq 1$ is a decreasing integer sequence (why?)

Thus, the algorithm will always terminate.

Now suppose that the algorithm has terminated at step i, and set $c = r_i$.

We prove that $c = \gcd(a,b)$. To do so, it suffices to show that

(i) c is a common divisor, i.e. c divides a and b

(ii) If d is any common divisor, then $d \leq c$.

For (i), we work through the algorithm backward, and show that c divides r_j for $j = i, i-1, \dots, 1, 0$. Indeed,

- $r_i = c \Rightarrow$ c divides r_i
- $r_{i-1} = q_{i+1} r_i + \underbrace{r_{i+1}}_{=0 \text{ because of termination}} \Rightarrow$ c divides r_{i-1}
- $r_{i-2} = q_i \underbrace{r_{i-1}}_{c \text{ divides}} + \underbrace{r_i}_{c \text{ divides}} \Rightarrow$ c divides r_{i-2}

$\vdots$

- $r_0 = q_2 r_1 + r_2 \Rightarrow$ c divides r_0

For (ii), we work through the algorithm forward. Suppose that d is a common divisor. We show that d divides r_j for $j = 0, 1, \dots, i$. Indeed,

- $r_0 = a \Rightarrow$ d divides r_0
- $r_1 = b \Rightarrow$ d divides r_1
- $r_0 = q_2 r_1 + r_2 \Rightarrow r_2 = r_0 - q_2 r_1 \Rightarrow$ d divides $r_2 \neq 0$ (unless already terminated)

$\vdots$

- $r_{i-2} = q_i r_{i-1} + r_i \Rightarrow r_i = r_{i-2} - q_i r_{i-1} \Rightarrow$ d divides $r_i = c$

Since d divides c, $d \leq c$.

□