

$= 0$ ), the remainders  $r_{k+2}$  and  $r_{k+1}$  equal  $a$  and  $b$ , the numbers for which the GCD is sought. In the next step ( $k =$

$1$ ), the remainders equal  $b$  and the remainder  $r_0$  of the initial step, and so on. Thus, the algorithm can be written as a sequence of equations

<formula>

If  $a$  is smaller than  $b$ , the first step of the algorithm swaps the numbers. For example, if  $a < b$ , the initial quotient  $q_0$  equals zero, and the remainder  $r_0$  is  $a$ . Thus,  $r_k$  is smaller than its predecessor  $r_{k+1}$  for all  $k \geq 0$ .

Since the remainders decrease with every step but can never be negative, a remainder  $r_N$  must eventually equal zero, at which point the algorithm stops. The final nonzero remainder  $r_{N-1}$  is the greatest common divisor of  $a$  and  $b$ . The number  $N$  cannot be infinite because there are only a finite number of nonnegative integers between the initial remainder  $r_0$  and zero.

== Proof of validity ==