Here is an algorithm that takes as input two positive integers m and n and outputs an integer. (Recall that for numbers a, b, $\max(a, b)$ is the maximum of a and b and $\min(a, b)$ is the minimum of a and b.)

1 Let $g = \max(m, n)$.

2 Let $s = \min(m, n)$.

3 If s is a divisor of g then output s and stop.

4 Otherwise, let r be the remainder when g is divided by s.

5 Change the value of g to the value of s.

6 Change the value of s to the value of r.

7 Go to line 3.

Prove that this algorithm outputs the greatest common divisor of m and n.

Let the algorithm applied to two numbers, a, b be denoted $E(a, b)$. Since at lines $5 - 7$ the algorithm sets g to be the minimum, and s to be the remainder of the division between m, n, which makes it strictly less than n, therefore having $g = max(n, r), s = min(s, r)$ is the same as evaluating $E(n, r)$, therefore $E(m, n) = E(min(m, n), r)$.

We must show that this algorithm finds the gcd. By definition of the algorithm we must show $E(m, n) = gcd(m, n)$. By the principal of mathematical induction for all $j, k \in \mathbb{N}$ if $j, k < max(m, n)$, then $E(j, k) = \gcd(j, k)$. Suppose $m, n \in \mathbb{N}$. Without loss of generality let $m = max(m, n), n = min(m, n)$. We must show that $E(m, n) = gcd(m, n)$. We have two cases, $n \mid m, n \nmid m$.

- Assume $n \mid m$. Then $m = np, p \in \mathbb{N}$. Therefore the algorithm terminates on the first pass on the third line, and $E(m, n) = n$. Since between n, m, n is the largest factor, then $gcd(m, n) = n$. Therefore $E(m, n) = gcd(m, n)$.
- Assume $n \nmid m$. By the quotient remainder theorem there exists $q, r \in Z, 0 < r < n$ such that $m = qn + r$. Then applying a first pass of the algorithm lines $1 - 7$ to m, n yields $E(m, n) = E(n, r)$. By the induction hypothesis we have that $E(n, r) = \gcd(n, r)$. Therefore we must show $\gcd(n, m) = \gcd(n, r)$. Let $l = \gcd(n, r)$. Therefore by the definition of $\gcd, l \mid n, l \mid r$. By definition of divisibility $ln' = n, lr' = r$. Therefore $l(qn' + r') = qn + r = m$. By definition of divisibility $lm' = m, m' \in \mathbb{Z}$. Therefore by definition of divisibility $l \mid m$. By definition of $\gcd(n, r) = l$ there exists $x_1, x_2 \in \mathbb{Z}$ such that $nx_1 + rx_2 = l$. By definition of $r = m - nq$, we have that $(x_1 - qx_2)n + x_2m = l$. Dividing both sides by l yields $(x_1 - qx_2)n' + x_2m' = 1$. Therefore by definition $\gcd(n', m') = 1$. Therefore l is the greatest common factor between m, n. Thus $\gcd(n, r) = \gcd(m, n)$.

Therefore the requirements have been satisfied.