Inductive proof of Euclid's Algorithm for the BCD

Euclid's algorithm is based on the principle that the GCD of two numbers does not change if the larger number is replaced by its difference with the smaller number. Here's how you can prove it:

1. **Statement of the Algorithm**:
   - Given two positive integers m and n where $m \geq n$, the algorithm repeatedly replaces m by $m \mod n$ (the remainder when m is divided by n) until $m = 0$. The non-zero remainder at this stage is the GCD of m and n.
2. **Proof by Induction**:
   a. **Base Case**:
   - If $n = 0$, the GCD of m and n is m by definition, because any number is divisible by 0.
   - If $m \mod n = 0$, then n divides m perfectly, so the GCD is n.

   b. **Inductive Step**:
   - Assume the algorithm correctly finds the GCD for two numbers m' and n' where $m' < m$ and $n' < n$.
   - Now, consider the original pair m and n. The algorithm performs the step $m \mod n = r$, where r is the remainder. According to the algorithm, the next step is to compute the GCD of n and r.
   - By the division algorithm, we have:

     $$m = q \cdot n + r$$

     where q is the quotient and $r = m \mod n$.
   - The GCD of m and n is the same as the GCD of n and r because any common divisor of n and r must also divide m.
   - Therefore, by the inductive hypothesis, the algorithm correctly computes the GCD of n and r, and hence also the GCD of m and n.
3. **Conclusion**:
   - By the principle of mathematical induction, Euclid's algorithm correctly computes the GCD of any two positive integers m and n.