A Better Proof of GCD3

1. SUFFICES ASSUME: m, n, and d are integers
   PROVE: d divides both m and n iff d divides both m and $n - m$

   PROOF: Since the gcd of two numbers is the largest integer that divides both of them, it suffices to show that m and n have the same common divisors as m and $n - m$.

2. ASSUME: d divides both m and n
   PROVE: d divides both m and $n - m$

   PROOF: That d divides m follows by the assumptions; that it divides $n - m$ follows from the assumptions and Lemma Div.

3. ASSUME: d divides both m and $n - m$
   PROVE: d divides both m and n

   PROOF: That d divides m follows from the assumptions; that it divides n follows from the assumptions, Lemma Div, and the simple algebraic relation: $n = m + (n - m)$.

4. Q.E.D.

   PROOF: By 1, 2, and 3.

CLOSE