Math 161 Modern Geometry Homework Questions 1 (part 2)

5) We just prove the algorithm works, i.e. it produces the greatest common divisor of a, b. Suppose algorithm produces the sequence $(r_1, r_2, \ldots, r_n, r_{n+1} = 0)$ for some $n \geq 1$ such that:
$a = q_1 b + r_1$, $0 \leq r_1 < b$,
$b = q_2 r_1 + r_2$, $0 \leq r_2 < r_1$,
....
$r_{n-1} = q_{n+1} r_n + r_{n+1}$.

We claim that r_n is the $gcd(a, b)$. Recall $a \geq b > 0$.

First note the following easy fact: if c divides d and c divides $f - kd$ for any integer k, then c divides f. (Think about why this is true).

Claim 1: r_n is a common divisor of a, b.

Proof. We work backwards from the last equation up to the first equation. The last equation tells us: r_n divides r_{n-1}.

The second-to-last equation is: $r_{n-2} = q_n r_{n-1} + r_n$. So we get $r_n = r_{n-2} - q_n r_{n-1}$ so indeed, r_n divides $r_{n-2} - q_n r_{n-1}$. The observation above tells us r_n divides r_{n-2}.

By induction (or simply proceed as above), we get that r_n divides b (using the second equation). Using the first equation, we again get r_n divides a. □

Claim 2: Suppose s is a common divisor of a, b. Then s divides r_n.

Proof. In the previous claim, we worked backwards (from the last equation up). Now we work downwards.

First equation: since s is a common divisor of a, b, s also divides $a - q_1 b = r_1$.

Second equation: since s divides both r_1, b, s divides $q - q_2 r_1 = r_2$.

....

Second-to-last equation: since s divides r_{n-2}, r_{n-1}, s divides $r_{n-2} - q_n r_{n-1} = r_n$. □

The two claims imply that r_n is $gcd(a, b)$.