

SOLUTIONS TO HOMEWORK 3
Math 104 - Dr. Evans
UCSD Winter 2004

1. Let a and b be two positive integers. Suppose repeated applications of the Euclidean algorithm results in the following set of equations:

$$\begin{array}{lll} (1) & a = b \cdot q_1 + r_1 & 0 < r_1 < b \\ (2) & b = r_1 \cdot q_2 + r_2 & 0 < r_2 < r_1 \\ (3) & r_1 = r_2 \cdot q_3 + r_3 & 0 < r_3 < r_2 \\ (4) & r_2 = r_3 \cdot q_4 + r_4 & 0 < r_4 < r_3 \\ (5) & r_3 = r_4 \cdot q_5 + 0 & \end{array}$$

Prove that r_4 is the greatest common divisor of a and b .

First we prove a lemma.

Lemma 1. If $d|r$ and $d|s$, then $d|xr + ys$ for any integers x and y .

Proof. If $d|r$, then by definition there exists an integer k such that $r = kd$. Likewise, if $d|s$, then by definition there exists an integer l such that $s = ld$. Hence, $xr + ys = x(kd) + y(ld) = d(xk + yl)$. Since $xk + yl$ is an integer, we have $d|(xr + ys)$ by definition of divisibility.

To prove that r_4 is the greatest common divisor of a and b , we first show that r_4 is a common divisor of a and b . By the equation (5), $r_3 = r_4 \cdot q_5$ implies that $r_4|r_3$. Equation (4) show that r_2 is a linear combination of r_3 and r_4 . Since $r_4|r_3$ and $r_4|r_4$, Lemma 1 shows that $r_4|r_2$. The exact same argument shows that $r_4|r_1$, $r_4|b$, and $r_4|a$. Therefore, r_4 is a common divisor of a and b .

We now show that r_4 is the *greatest* common divisor by showing that every other common divisor of a and b also divides r_4 . Suppose $d|a$ and $d|b$. Rearranging equation (1) results in $r_1 = a - b \cdot q_1$. Since r_1 is a linear combination of a and b , Lemma 1 shows that $d|r_1$. Going down the list of equations, we can solve for r_2 , r_3 , and r_4 as linear combinations of the previous remainders. Lemma 1 shows that $d|r_2$, $d|r_3$, and $d|r_4$, respectively. Therefore, r_4 satisfies the two conditions of being the greatest common divisor of a and b .

Another valid proof is to start by proving that $\gcd(a, b) = \gcd(a + kb, b)$ for any integer k . It is enough to show that every common divisor of a and b is a common divisor of $a + kb$ and b , and vice versa. One could prove this directly, or apply Lemma 1. Once this is established, then the theorem following quickly. Since $r_1 = a - b \cdot q_1$, we have $\gcd(a, b) = \gcd(b, r_1)$. The same argument for each successive remainder shows that

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \gcd(r_3, r_4) = r_4$$

since $r_4|r_3$.