Math 4330, Homework 5 Solutions [1]

1. Show that if $u > v$ then $(u \bmod v) \leq u/2$.
Solution: Case I: If $v \leq u/2$, then since $(u \bmod v) < v$, it follows immediately that $(u \bmod v) < v \leq u/2$.
Case II: Suppose $v > u/2$, and write $u = qv + r$ with $q, v \in \mathbb{Z}$ and $0 \leq r < v$. Since $u/v < 2$, it follows that $q < 2$, so we must have $q = 1$ (we are implicitly assuming both u and v to be positive, since that's all we've considered in class). Therefore, $(u \bmod v) = r = u - qv = u - v < u - u/2 = u/2$.

---

2. Use the previous result to prove that in Algorithm A, Step A2 is executed no more than $1 + 2\log_2 u$ times. (In particular, it follows that the Euclidean Algorithm is *polynomial-time* in the input size which is $\log_2 u + \log_2 v$.)
Solution: Let u_j denote the value of the variable u just prior to the j-th time Step A2 is executed, and let v_j be similarly defined. Then $u_1 = u$, $v_1 = v$, and Step A2 is executed exactly k times, where k is the least non-negative integer for which $v_k = 0$.

If the initial inputs u and v satisfy $u \leq v$, then we'll have $u_1 \leq v$. However, for all $j \geq 2$ we'll have $u_j > v_j$. Furthermore, if $v_j \neq 0$, then we have after the j-th iteration of Step A2 that

$$u_{j+1} = v_j, \quad \text{and} \quad v_{j+1} = (u_j \bmod v_j)$$

We have that $u_{j+2} = v_{j+1}$ and it follows from Problem 1 that $v_{j+1} \leq u_j/2$, and thus, $u_{j+2} \leq u_j/2$. From this, we have that $u_3 \leq u_1/2$, $u_5 \leq u_3/2 \leq u_1/2^2$, and in general, $u_{1+2m} \leq u_1/2^m$. For $m > \log_2 u$ we obtain

$$u_{1+2m} \leq \frac{u_1}{2^m} < \frac{u_1}{2^{\log_2 u}} = \frac{u_1}{u} \leq 1,$$

which would imply that $u_{1+2m} = 0$. By assumption, the algorithm terminates after the k-th iteration of Step 2 and we have $u_k > v_k = 0$, so $k < 1 + 2\log_2 u$.