CCS Discrete Math I Professor: Padraic Bartlett

Homework 10: The Euclidean Algorithm!

Due Friday, Week 5 *UCSB 2014*

Do **one** of the **two** problems below!

These problems are both centered around the **Euclidean algorithm**, which is a method for taking two positive integers $a > b$ and calculating their GCD:

Algorithm. To initialize our algorithm, set $r_1 = a, r_2 = b$. Our algorithm will create a sequence of values $r_1, r_2, r_3 \ldots r_k,$, where this last value r_k will be the GCD of a, b.

1. Suppose that we have defined our sequence up to r_i, r_{i+1}, that $r_i > r_{i+1}$, and that $r_{i+1} > 0$.
2. If the remainder of r_i when divided by r_{i+1} is 0, quit our algorithm: r_{i+1} is the GCD we were looking for.
3. Otherwise, to define r_{i+2}, simply set it equal to the remainder of r_i when divided by r_{i+1}. This always gives us a number smaller than r_{i+1} that is positive, by definition.
4. Go to 1.

We give an example run of this algorithm for the two values $63, 99$:

1. Set $r_1 = 99, r_2 = 63$.
2. The remainder of 99 divided by 63 is 36; so set $r_3 = 36$.
3. The remainder of 63 divided by 36 is 27; so set $r_4 = 27$.
4. The remainder of 36 divided by 27 is 9; so set $r_5 = 9$.
5. The remainder of 27 divided by 9 is 0; so our algorithm quits, and says that the GCD of 63 and 99 is 9.

The algorithm works here, as we can check: because $63 = 9 \cdot 7$ and $99 = 9 \cdot 11$, the GCD of 63 and 99 is 9, as claimed!

1. Prove that this algorithm does work! In other words, show that the GCD of any two numbers a, b can be calculated by the above process.
2. Using the algorithm above, prove the following result:

   Theorem. If a, b are two positive integers, then we can find two more integers n, m such that

   $$na + mb = GCD(a, b).$$