WORKSHEET #1 – MATH 311W

AUGUST 29TH, 2012

In this worksheet our goal is to understand (and prove) the Euclidean algorithm. We assume you have covered up through page 8 in the text.

We begin with a Lemma.

Lemma: *Suppose that $a > 0$ and $b > 0$ are integers. Further suppose we write*

$$b = aq + r$$

for some integers q and $r \geq 0$ (we do NOT *assume that $r < a$ but that case works too). Then* $\gcd(a, b) = \gcd(a, r)$.

We will prove this lemma in steps.

(1). Suppose that $d = \gcd(a, b)$. Prove that $d|r$ and thus conclude that $d|\gcd(a, r)$.

Hint: Use the fact that $a = md$ and and $b = nd$ (for some m, n) to conclude that $r = od$ for some o.

(2). Suppose that $e = \gcd(a, r)$. Prove that $e|b$ and conclude that $e|\gcd(a, b)$.

(3). Combine parts 1. and 2. to conclude that $\gcd(a, b) = d = e = \gcd(a, r)$ which proves the lemma.

The Euclidean algorithm is an algorithm which can find the gcd of any two numbers, a and b.

Algorithm: *Given integers* $a > 0, b > 0$*, we will compute* $\gcd(a, b)$*. Write*

$$b = aq_1 + r_1 \textit{ for some integers } q_1 > 0 \textit{ and } a > r_1 \geq 0.$$

If $r_1 = 0$ **STOP**. *Otherwise, write*

$$a = r_1 q_2 + r_2 \textit{ for some integers } q_2 > 0 \textit{ and } r_1 > r_2 \geq 0.$$

If $r_2 = 0$ **STOP**. *Otherwise, write*

$$r_1 = r_2 q_3 + r_3 \textit{ for some integers } q_2 > 0 \textit{ and } r_2 > r_3 \geq 0.$$

If $r_3 = 0$ **STOP**. *Otherwise, write*

$$r_2 = r_3 q_4 + r_4 \textit{ for some integers } q_3 > 0 \textit{ and } r_3 > r_4 \geq 0.$$

If $r_4 = 0$ **STOP**. *Otherwise, write*

....

In general, if $r_n = 0$ *STOP. Otherwise write*

$$r_{n-1} = r_n q_{n+1} + r_{n+1} \textit{ for some integers } q_{n+1} > 0 \textit{ and } r_n > r_{n+1} \geq 0.$$

(4). Show that $\gcd(b, a) = \gcd(a, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots = \gcd(r_n, r_{n+1})$ by using the Lemma.

(5). We must show that this algorithm eventually terminates. Suppose it didn't, and then consider the set of positive integers $\{r_1, r_2, r_3, r_4, \ldots\}$. Use the well ordering principal to obtain a contradiction.

(6). Explain what you should do when you get to a **STOP** in order to find the gcd.

(EXTRA CREDIT) In any computer language or scripting language of your choice, implement the Euclidean algorithm. Then turn in your *commented* source code with examples of it running. If you are not familiar with a computer or scripting language, write a 1-2 page paper explaining how a *recursive* algorithm could be used to find the gcd. (You will probably need to look up *"recursive algorithm"*). Due Wednesday, September 5th. (Worth 3 points to your homework score).