SECTION 5.5 AND SECTION 6.1

DAVID SEAL

5–5, #13

The loop invarient for the Euclidean algorithm is given by the fact that each time we update the local variables x and y, the gcd's stay the same. That is, $p =$ "$\gcd(a,b) = \gcd(x,y) \wedge y \geq 0$" is a loop invariant. The condition terminates when $y = 0$, provided it actually gets there.

When we enter the loop, p is obviously true since x and y get set to a and b respectively. If we divid y into x, we get

$$x = qy + r,$$

for some $q, r \in \mathbb{Z}$. Because $\gcd(m,n) = \gcd(n,r)$ for any $m, n, q, r \in \mathbb{Z}$ which satisfy $m = nq + r$, we know that $\gcd(x,y) = \gcd(y,r)$. This implies that $\gcd(a,b) = \gcd(y,r)$. The content of the while loop replaces x with y and y with r, and therefore p is an invariant, since it will be true at the end of the while loop.

To verify the correctness, we need to make sure that y eventually hits zero. After the first pass, we can assume that $y < x$. The first pass may simply swap x and y. The division algorithm gaurantees that $0 \leq r < y$, so we know that y decreases by at least 1. This tells us that we can remain inside the loop for *at most* b steps, and therefore we will eventually terminate.

The reason we terminate is that $y = 0$. Because $\gcd(x,0) = x$ for any $0 \neq x \in \mathbb{Z}$, we know that $x = \gcd(a,b)$ when the algorithm terminates.

□

6–1, #17 There are a couple of ways to solve this problem. I think the shortest is the following. Consider $A = \{$words with at least 1 @ symbol$\}$, and $B = \{$words with no @ symbols$\}$, both subsets of words of length 5.

Obviously $|B| = 127^5$ since we remove exactly one character from the alphabet. Also $|A \cup B| = 128^5$, since this covers all possible words of length 5 and $A \cap B = \emptyset$. Inclusion/exclusion gives

$$|A \cup B| = |A| + |B| - |A \cap B| = |A| + |B|$$

which means $|A| = 128^5 - 127^5$

Mike pointed out that we can count words with exactly 1, 2, 3, 4 and 5 @ characters in them. This gives

$$|A| = 5 \cdot 127^4 + 10 \cdot 127^3 + 10 \cdot 127^2 + 5 \cdot 127 + 1.$$

The first term is the number of words with exactly 1 @ symbol. The second term is the number of words with exactly 2 @ symbols, etc.

□