COL765
Quiz 1 solutions

Problem 1:

Haskell program

```
mod a b = if a < b then a else mod (a–b) b
```

Proof of correctness

Induction on a.
Base case: $a < b$, consider $a = 0$. Then $mod\ a\ b = a = 0 = bq + r \implies q = 0, r = 0$.
I.H.: Assume for all $0 \leq k < a$ we have that $k = bq' + r'$ (or $mod\ k\ b = r$).
I.S.: Assume $0 < a = m = bq + r$.

Case 1: $a < b$; then $a = 0q + r = a = mod\ a\ b$ (by defn.)

Case 2: $a \geq b$, then by defn. $mod\ a\ b = mod\ (a - b)\ b$. Since $b > 0$, we have $a - b < a$. Apply I.H. on $mod\ (a - b)\ b$, we have that for some q, r: $a - b = bq + r \implies a = (q + 1)b + r$ thus $mod\ (a - b)\ b = r$

Problem 2:

Haskell program

```
mul a 0 = 0
mul 0 b = 0
mul a b = add a (mul a (b−1))
```