Homework 8

Due midnight, Thursday, 4/2/2015

Please submit your homework solutions online at `http://www.dci.pomona.edu/tools-bin/cs081upload.php`. If you have more than one file to be turned in, please put it in a folder and zip it up before turning it in.

1. (10 points) **Program Proofs**

   Problem 4.3.13 from H & R page 301. Please show the proof carefully in the same style as the proof in Example 4.17 on page 286. *Hint: Consider a loop invariant of* $x == y{+}a$.

   Be careful to use the Imply rule in the correct direction. In the past many students have lost points by proving implications in the wrong direction!

2. (15 points) **More program proofs**

   This exercise is about integer division. Suppose that a and b are positive integers. If we divide a by b we get a quotient q and a remainder r satisfying

   $a = bq + r$ and $0 \leq r < b$.

   We use Python/Java/C notation for the remainder, $a \,\%\, b$. We say that b *divides* a, written $b|a$, if the remainder is zero. Notice that $b|a$ implies $b \leq a$.

   Further, a number d divides both a and b if and only if d divides both b and r.

   The *greatest common divisor* of a and b, written $\gcd(a, b)$, is the largest element of the set $\{d \mid 0 < d,\ d|a, \text{ and } d|b\}$.

   (a) Annotate the block of code in Figure 1 to verify that it is a correct Hoare triple. A full box-and-line proof is not necessary; just annotate each step and give a brief reason why the annotation is correct.

$\{0 < B < A\}$

```
a := A;
b := B;
while (0 < b) {
   t := a;
   a := b;
   b := t % b;
}
```

$\{\mathtt{b} = 0 \wedge \forall d\, \big(0 < d \to \big(d|\mathtt{a} \wedge d|\mathtt{b} \leftrightarrow d|A \wedge d|B\big)\big)\}$

Figure 1: An instance of Euclid's algorithm to compute greatest common divisors.

   Until now, we have avoided using the symbol for logical equivalence. The notation $\phi \leftrightarrow \psi$ is an abbreviation for $(\phi \to \psi) \wedge (\psi \to \phi)$.

   (b) Argue informally that the postcondition implies $\mathtt{a} = \gcd(A, B)$.

3. (10 points) **Program Proofs**

   Problem 4.4.1a from H & R page 303.