

Homework Solutions - Section 4.1

9.

(a) Before the loop, $m + n$ is even.

After the loop:

$$m' = m + 1$$

$$n' = n + 1$$

$$m' + n' = (m + 1) + (n + 1) = m + n + 2 \text{ which is also even}$$

(b) Before the loop, $m + n$ is odd .

After the loop:

$$m' = m + 1$$

$$n' = n + 1$$

$$m' + n' = (m + 1) + (n + 1) = m + n + 2 \text{ which is also odd}$$

11.

(a)

Given $i < j^2$ before the loop with $n = 1$,

To enter the loop, $j \geq 1$; thus, after the loop:

$$i' = i + 2$$

$$j' = j + 1$$

Hence, with $j \geq 1$

$$i' = i + 2 < j^2 + 2 < j^2 + 2j + 1 = (j + 1)^2 = j'^2$$

Therefore, $i < j^2$ is a loop invariant.

(b)

Given $0 \leq i < j^2$ before the loop with $n = 0$,

Since the case $i < j^2$ with $j = 0$ can not occur, $j \geq 1$ and part (a) applies.

Therefore, $0 \leq i < j^2$ is a loop invariant

(c)

Given $i \leq j^2$ before the loop with $n = 0$,

Let $i = j = 0$ before the loop.

Then,

$$i' = i + 2 = 2 \not\leq j'^2 = (j + 1)^2 = 1$$

Hence, $i \leq j^2$ is not a loop invariant.

(d)

Given $i \geq j^2$ before the loop with $n = 0$,

Let $i = j = 1$ before the loop.

Then,

$$i' = i + 2 = 3 \not\geq j'^2 = (j + 1)^2 = 4$$

Hence, $i \geq j^2$ is not a loop invariant.

17.

(a) $r < 73$ is a loop invariant by definition of MOD 73.

(b) Given $r \equiv 0 \pmod{5}$

Let $r = 5$, then $r' = 31 \cdot r \text{ MOD } 73 = 155 \text{ MOD } 73 = 9 \not\equiv 0 \pmod{5}$

Hence, $r \equiv 0 \pmod{5}$ is not a loop invariant

(c) $r = 0$ is a loop invariant vacuously (you never enter the loop)

19.

(a) yes

(b) no - because $\mathbb{Z} \not\subseteq \mathbb{N}$

(c) yes

(d) no - because $\{n \in \mathbb{Z} : n^2 > 17\} \not\subseteq \mathbb{N}$

(e) no - $\{n \in \mathbb{P} : n^2 < 0\} = \emptyset$

(f) yes

21.

(a) "a, b, and r are multiples of 5"

After the loop, with $r > 0$:

$$a' = b \text{ (clearly a multiple of 5)}$$

$$b' = r \text{ (clearly a multiple of 5)}$$

$$r' = a' \text{ MOD } b' = b \text{ MOD } r$$

Now, since $b = (b \text{ DIV } r) \cdot r + (b \text{ MOD } r)$,

$$r' = b \text{ MOD } r = (b \text{ DIV } r) \cdot r - b \text{ which is a multiple of 5}$$

Hence, "a, b, and r are multiples of 5" is a loop invariant.

(b) "a is a multiple of 5"

Let $r = 1$ and $b = 3$, then $a' = 3$ which is not a multiple of 5.

Thus, "a is a multiple of 5" is not a loop invariant

(c) " $r < b$ "

After the loop, $r' = a' \text{ MOD } b' = b \text{ MOD } r < r = b'$

Hence, " $r < b$ " is a loop invariant

(d) " $r \leq 0$ "

This is an invariant vacuously - we never enter the loop.