Problem 3

We show that

$$I: \begin{array}{l} x \geq 0 \text{ and } y \geq 0 \\ \forall d > 0 (d | x \text{ and } d | y \text{ iff } d | a \text{ and } d | b). \end{array}$$

is the loop invariant.

Claim: Initialization: $P \Rightarrow I$.

Proof: The pre-conditions are $x = a$ and $y = b$. By the requires clause, $x = a > 0$ and $y = b > 0$. Thus

$$x \geq 0 \text{ and } y \geq 0 .$$

Also,

$$d | a \text{ and } d | b \text{ iff } d | a \text{ and } d | b$$

$$d | x \text{ and } d | y \text{ iff } d | a \text{ and } d | b .$$

Thus I holds. $\square$

Claim: Preservation: $\{I \wedge B\}\ S\ \{I\}$.

Proof:

$P(k)$: For all iterations $k \geq 1$ of the loop, I holds before and after iteration k.

Base Case: $k=1$

We've already shown that $P \Rightarrow I$. So I holds before the first iteration.

After the first iteration

$$temp := y = b$$
$$y := x \% y = a \% b$$
$$x = temp = b$$

So $x = b$ and $y = a \% b$. By the requires clause, $x = b > 0$ so $x \geq 0$.

By the requires clause again, $a, b > 0$.

The $\%$ operation returns the remainder r of a divided by b with r having the same sign as a. Since $a > 0$ (this is the requires clause),

$$y = a \% b = r > 0 .$$

Thus

$$x \geq 0 \text{ and } y \geq 0 .$$

We now show that

$$\forall d > 0 \, (d|x \text{ and } d|y \iff d|a \text{ and } d|b).$$

$(\Rightarrow)$: After the first iteration, $x = b$ and $y = a \% b$.

Assume $d > 0$ and $d|x$ and $d|y$. That is, $d|b$ and $d|a \% b$. Now $a \% b$ is the remainder r of a divided by b. Since $d|r$, we have

$$a = bq + r$$
$$= bq + kd$$

for some $k \in \mathbb{Z}$. Since $d \mid b$, we have

$$a = bq + kd$$
$$= k_1 dq + kd$$
$$= d(k_1 q + k) \quad .$$

Thus $d \mid a$ and $d \mid b$. $\boxed{\mapsto}$

($\Leftarrow$): Assume $d > 0$ and $d \mid a$, $d \mid b$. We need to show $d \mid x$ and $d \mid y$. After iteration 1

$$x = b$$
$$y = a \% b \quad .$$

Since $d \mid b$, we have $d \mid x$.

$$a = bq + r = (dk)q + r$$

Since $d \mid a$, we have

$$a = k_1 d = kdq + r$$
$$r = k_1 d - kdq$$
$$= d(k_1 - kq)$$

where $r = a \% b = y$. Thus $d \mid y$. So

$$d \mid y \text{ and } d \mid x. \quad \boxed{\rightarrow}$$

This tells us that the invariant

- $\forall d > 0 \, (d \mid x \text{ and } d \mid y \text{ iff } d \mid a \text{ and } d \mid b)$
- $x \geq 0$ and $y \geq 0$

holds after the first iteration, as well as before it.

Induction hypothesis (IH): Assume I holds befor and after the k^{th} iteration $\forall k \geq 1$.

Induction Step (IS): We need to show that I holds before the k+1 iteration and after it. That is,

$$X_{B_{k+1}} \geq 0 \quad \text{and} \quad Y_{B_{k+1}} \geq 0$$

(Before k+1 iteration):

$$d \mid X_{B_{k+1}} \text{ and } d \mid Y_{B_{k+1}} \text{ iff } d \mid a \text{ and } d \mid b \quad \forall d > 0.$$

$$X_{A_{k+1}} \geq 0 \quad \text{and} \quad Y_{A_{k+1}} \geq 0$$

(After k+1 iteration):

$$d \mid X_{A_{k+1}} \text{ and } d \mid Y_{A_{k+1}} \text{ iff } d \mid a \text{ and } d \mid b \quad \forall d > 0.$$

Before the k+1 iteration

$$X_{B_{k+1}} = X_{A_k} = \underbrace{Y_{A_k} \geq 0}_{\text{By the IH}}$$

$$Y_{B_{k+1}} = Y_{A_k} = X_{B_k} \,\%\, Y_{B_k}$$

By the IH, $X_{B_k} \geq 0$ and $Y_{B_k} \geq 0$. Thus $X_{B_k} \% Y_{B_k} \geq 0$. So

$$Y_{B_{k+1}} \geq 0 .$$

We now show that

$$d \mid x_{B_{k+1}} \text{ and } d \mid y_{B_{k+1}} \text{ iff } d \mid a \text{ and } d \mid b \quad \forall d > 0.$$

Assume $d > 0$.

$(\Rightarrow)$: Assume $d \mid x_{B_{k+1}}$ and $d \mid y_{B_{k+1}}$.

Now

$$x_{B_{k+1}} = x_{A_k} = y_{B_k} = y_{A_{k-1}}$$

So $d \mid y_{B_k}$. Now

$$y_{B_{k+1}} = y_{A_k} = x_{B_k} \% y_{B_k} = r$$

where r is the remainder of x_{B_k} divided by y_{B_k}. So

$$x_{B_k} = q * y_{B_k} + r$$

Since $d \mid y_{B_k}$, $y_{B_k} = pd$. So

$$x_{B_k} = pd\, y_{B_k} + r$$

We assumed that $d \mid y_{B_{k+1}}$, i.e., $d \mid r$. So $r = gd$.

$$x_{B_k} = dp\, y_{B_k} + gd$$
$$= d(p\, y_{B_k} + g).$$

So $d \mid x_{B_k}$. So we have

$$d \mid x_{B_k} \text{ and } d \mid y_{B_k}. \quad (1)$$

By the IH, we know

$$d \mid x_{B_k} \text{ and } d \mid y_{B_k} \text{ iff } d \mid a \text{ and } d \mid b \quad (2).$$

Thus (1) and (2) give

$$d \mid a \text{ and } d \mid b. \quad \boxed{\rightarrow}$$

($\Leftarrow$): The reverse direction argument is very similar to the argument for the forward direction.

We have shown that I holds before iteration $k+1$. That is,

$$\begin{pmatrix}\text{Before } k+1 \\ \text{iteration}\end{pmatrix}: \quad \begin{array}{l} X_{B_{k+1}} \geq 0 \quad \text{and} \quad Y_{B_{k+1}} \geq 0 \\ d \mid X_{B_{k+1}} \text{ and } d \mid Y_{B_{k+1}} \text{ iff } d \mid a \text{ and } d \mid b \quad \forall d > 0. \end{array}$$

We now show that I holds after the $k+1$ iteration. That is,

$$\begin{pmatrix}\text{After } k+1 \\ \text{iteration}\end{pmatrix}: \quad \begin{array}{l} X_{A_{k+1}} \geq 0 \quad \text{and} \quad Y_{A_{k+1}} \geq 0 \\ d \mid X_{A_{k+1}} \text{ and } d \mid Y_{A_{k+1}} \text{ iff } d \mid a \text{ and } d \mid b \quad \forall d > 0. \end{array}$$

<u>Claim:</u> $X_{A_{k+1}} \geq 0$ and $Y_{A_{k+1}} \geq 0$

$$X_{A_{k+1}} = Y_{B_{k+1}} \geq 0$$

This last inequality is implied by the proof of I holding before the $k+1$ iteration.

$$Y_{A_{k+1}} = X_{B_{k+1}} \% Y_{B_{k+1}}$$

We know that $X_{B_{k+1}} \geq 0$ (I holds before $k+1$), thus the sign of

$$X_{B_{k+1}} \% Y_{B_{k+1}}$$

will be +ve. Hence $Y_{A_{k+1}} = X_{B_{k+1}} \% Y_{B_{k+1}} \geq 0$. This proves the claim.

We now prove

Claim: $d \mid x_{A_{k+1}}$ and $d \mid y_{A_{k+1}}$ iff $d \mid a$ and $d \mid b$ $\quad \forall d > 0$.

Let $d > 0$.

$(\rightarrow)$: Assume $d \mid x_{A_{k+1}}$ and $d \mid y_{A_{k+1}}$.

$$x_{A_{k+1}} = y_{B_{k+1}}.$$

So $d \mid y_{B_{k+1}}$.

$$y_{A_{k+1}} = x_{B_{k+1}} \% \, y_{B_{k+1}} = r$$

where r is the remainder of $x_{B_{k+1}}$ divided by $y_{B_{k+1}}$.

$$x_{B_{k+1}} = y_{B_{k+1}} * q + r$$

We know $d \mid y_{B_{k+1}}$ and $d \mid r$ (this is because $r = y_{A_{k+1}}$).
Thus $d \mid x_{B_{k+1}}$. We have

$$d \mid x_{B_{k+1}} \text{ and } d \mid y_{B_{k+1}} \quad . (1)$$

We know that I holds before iteration $k+1$, that is

$$d \mid x_{B_{k+1}} \text{ and } d \mid y_{B_{k+1}} \text{ iff } d \mid a \text{ and } d \mid b \quad . (2)$$

By (1) and (2) we get

$$d \mid a \text{ and } d \mid b. \qquad \boxed{\rightarrow}$$

The proof for the reverse direction is very similar, because this proof is already very lengthy I am skipping the proof of $(\leftarrow)$.

By induction, we have that $P(k)$ is true for all $k \geq 1$.

$\square$

Claim: Termination: $I \wedge \neg B \to Q$.

Proof: Assume $I \wedge \neg B$. That is

I:
- $x \geq 0$ and $y \geq 0$
- $\forall d > 0 \, (d \mid x$ and $d \mid y$ iff $d \mid a$ and $d \mid b)$.

and $y = 0$.

We show that

(1) • $gcd > 0$
(2) • $a \,\%\, gcd = 0$ and $b \,\%\, gcd = 0$
(3) • $d \mid a$ and $d \mid b \Rightarrow d \leq gcd$ for all $d > 0$.

(3) Assume $d \mid a$ and $d \mid b$ where $d > 0$. By I, $d \mid x$ and $d \mid y$. But $x = gcd$, so $d \mid gcd$. Hence

$$0 < d \leq gcd.$$

Which proves 3. $\boxed{3}$

(1) We know $gcd = x$. By I, $x \geq 0$. So $gcd \geq 0$.

To show (2), we know $gcd = x$. So we have to show

$$a \,\%\, x = 0 \text{ and } b \,\%\, x = 0.$$

I am not quite sure how to proceed.