

— Assignment 4 —  
**Program Verification**  
Sample Solution

---

### The Program *Totient*

```
t:=1;
x:=1;
while (n ≠ 1) do
  x:=x+1;
  if (x | n) then
    t:=t*(x-1);
    n:=n/x;
    while (x | n) do
      t:=t*x;
      n:=n/x
```

We will use the abbreviations *Loop1* for the main loop, *Body1* for the body of the main loop, *Condit* for the if statement and *Loop2* for the smaller loop nested inside.

## 1 Hoare Logic

Abbreviations for this section:

$$Inv1 \equiv (\varphi(N) = \varphi(n)t \wedge \forall y. (1 < y \leq x \rightarrow y \nmid n))$$

$$Inv2 \equiv (\varphi(N) = \frac{\varphi(nx)t}{x-1} \wedge \forall y. (1 < y < x \rightarrow y \nmid n) \wedge x \text{ is prime})$$

(i)  $\{Inv2\} Loop2 \{Inv1\}$

Our strategy is to start with the invariant *Inv2* as our postcondition, find the precondition of the body of *Loop2* (steps 1-3), use precondition strengthening to get it in the correct format for the while rule (4-5), apply the while rule (6), and then use postcondition weakening to derive our result (7-8).

1.  $\{\varphi(N) = \frac{\varphi(n)t}{x-1} \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime}\} n := n/x \{Inv2\}$  (Asst.)

2.  $\{\varphi(N) = \frac{\varphi(n)tx}{x-1} \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime}\} \mathbf{t} := \mathbf{t} * \mathbf{x}$   
 $\{\varphi(N) = \frac{\varphi(n)t}{x-1} \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime}\}$  (Asst.)
3.  $\{\varphi(N) = \frac{\varphi(n)tx}{x-1} \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime}\} \mathbf{t} := \mathbf{t} * \mathbf{x}; \mathbf{n} := \mathbf{n}/\mathbf{x}$   
 $\{Inv2\}$  (Seq. 1,2)
4.  $(Inv2 \wedge x \mid n) \rightarrow (\varphi(N) = \frac{\varphi(n)tx}{x-1} \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime})$   
(Facts 1,6)
5.  $\{Inv2 \wedge x \mid n\} \mathbf{t} := \mathbf{t} * \mathbf{x}; \mathbf{n} := \mathbf{n}/\mathbf{x} \{Inv2\}$  (Pre. Str. 3,4)
6.  $\{Inv2\} Loop2 \{Inv2 \wedge x \nmid n\}$  (While 5)
7.  $(Inv2 \wedge x \nmid n) \rightarrow Inv1$  (Facts 3,5,7)
8.  $\{Inv2\} Loop2 \{Inv1\}$  (Post. Weak. 6,7)

(ii)  $\{Inv1\} Body1 \{Inv1\}$

Given postcondition  $Inv1$ , steps 9-12 find the precondition for the body of the if statement *Condit*. Steps 13-15 put us in a position to use the conditional rule, which is Step 16. We finally push the argument through the first line of *Body1* to get our result (17-18).

9.  $\{\varphi(N) = \frac{\varphi(n)t}{x-1} \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime}\} \mathbf{n} := \mathbf{n}/\mathbf{x} \{Inv2\}$   
(Asst.)
10.  $\{\varphi(N) = \varphi(n)t \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime}\} \mathbf{t} := \mathbf{t} * (\mathbf{x} - 1)$   
 $\{\varphi(N) = \frac{\varphi(n)t}{x-1} \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime}\}$  (Asst.)
11.  $\{\varphi(N) = \varphi(n)t \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime}\}$   
 $\mathbf{t} := \mathbf{t} * (\mathbf{x} - 1); \mathbf{n} := \mathbf{n}/\mathbf{x} \{Inv2\}$  (Seq. 9,10)
12.  $\{\varphi(N) = \varphi(n)t \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime}\}$   
 $\mathbf{t} := \mathbf{t} * (\mathbf{x} - 1); \mathbf{n} := \mathbf{n}/\mathbf{x}; Loop2 \{Inv1\}$  (Seq. 11,8)
13.  $(\varphi(N) = \varphi(n)t \wedge \forall y. (1 < y < x \rightarrow y \nmid n) \wedge x \neq 1 \wedge x \mid n) \rightarrow$   
 $(\varphi(N) = \varphi(n)t \wedge \forall y. (1 < y < x \rightarrow y \nmid \frac{n}{x}) \wedge x \text{ is prime})$  (Facts 1,2)
14.  $\{\varphi(N) = \varphi(n)t \wedge \forall y. (1 < y < x \rightarrow y \nmid n) \wedge x \neq 1 \wedge x \mid n\}$   
 $\mathbf{t} := \mathbf{t} * (\mathbf{x} - 1); \mathbf{n} := \mathbf{n}/\mathbf{x}; Loop2 \{Inv1\}$  (Pre. Str. 12,13)
15.  $(\varphi(N) = \varphi(n)t \wedge \forall y. (1 < y < x \rightarrow y \nmid n) \wedge x \neq 1 \wedge x \nmid n) \rightarrow Inv1$  (Std. Math.)
16.  $\{\varphi(N) = \varphi(n)t \wedge \forall y. (1 < y < x \rightarrow y \nmid n) \wedge x \neq 1\} Condit \{Inv1\}$  (Cond. 14,15)
17.  $\{Inv1\} \mathbf{x} := \mathbf{x} + 1$   
 $\{\varphi(N) = \varphi(n)t \wedge \forall y. (1 < y < x \rightarrow y \nmid n) \wedge x \neq 1\}$  (Asst. + Simplifying)
18.  $\{Inv1\} Body1 \{Inv1\}$  (Seq. 16,17)

If you are confused about  $x + 1 \neq 1$  being simplified away during step 17, recall that all our variables are typed as positive non-zero integers.

(iii)  $\{n = N\}$  Totient  $\{t = \varphi(N)\}$

First we find the Hoare triple for *Loop1* (19-21). We then weaken the postcondition to get our desired result (22-23), and finally push the precondition through our first two lines of code, weakening appropriately to get the desired postcondition (24-29).

19. $(Inv1 \wedge n \neq 1) \rightarrow Inv1$	(Standard Logic)
20. $\{Inv1 \wedge n \neq 1\} Body1 \{Inv1\}$	(Pre. Str. 18,19)
21. $\{Inv1\} Loop1 \{Inv1 \wedge n = 1\}$	(While 20)
22. $(Inv1 \wedge n = 1) \rightarrow (t = \varphi(N))$	(Fact 4)
23. $\{Inv1\} Loop1 \{t = \varphi(N)\}$	(Post. Weak. 21,22)
24. $\{\varphi(N) = \varphi(n) t\} x := 1 \{Inv1\}$	(Asst. + Simplifying)
25. $\{\varphi(N) = \varphi(n)\} t := 1 \{\varphi(N) = \varphi(n) t\}$	(Asst.)
26. $(n = N) \rightarrow (\varphi(N) = \varphi(n))$	(Standard Math.)
27. $\{n = N\} t := 1 \{\varphi(N) = \varphi(n) t\}$	(Pre. Str. 25,26)
28. $\{n = N\} t := 1; x := 1 \{Inv1\}$	(Seq. 24,27)
29. $\{n = N\}$ Totient $\{t = \varphi(N)\}$	(Seq. 23,28)

## 2 Weakest Precondition Calculus

(i)  $P_0$  for  $wp(Loop1, t = 1)$

$$P_0 \equiv (n = 1 \wedge t = 1)$$

(ii)  $P_1$  for  $wp(Loop1, t = 1)$

First, we will tackle  $wp(Loop2, P_0)$ :

$$\begin{aligned}
Q_0 &\equiv x \not\equiv n \wedge P_0 \\
&\equiv x \neq 1 \wedge n = 1 \wedge t = 1 \\
Q_1 &\equiv x \mid n \wedge wp(t := t * x; n := n/x, Q_0) \\
&\equiv x \mid n \wedge wp(t := t * x, wp(n := n/x, Q_0)) \\
&\equiv x \mid n \wedge wp(t := t * x, x \neq 1 \wedge \frac{n}{x} = 1 \wedge t = 1) \\
&\equiv x \mid n \wedge x \neq 1 \wedge \frac{n}{x} = 1 \wedge tx = 1 \\
&\equiv \mathbf{False} \text{ because } tx = 1 \text{ implies } x = 1.
\end{aligned}$$

Therefore  $Q_k \equiv \mathbf{False}$  for  $k \geq 1$  because if a loop cannot terminate with a given postcondition after 1 step then it cannot terminate after any larger number of steps. Hence

$$\begin{aligned}
wp(\text{Loop2}, P_0) &\equiv \exists k. (k \geq 0 \wedge Q_k) \\
&\equiv (x \neq 1 \wedge n = 1 \wedge t = 1) \vee \mathbf{False} \vee \mathbf{False} \vee \dots \\
&\equiv (x \neq 1 \wedge n = 1 \wedge t = 1)
\end{aligned}$$

Now we can approach  $wp(\text{Body1}, P_0)$ . First we will look at the if statement *Condit*:

$$\begin{aligned}
wp(\text{Condit}, P_0) &\equiv (x \mid n \wedge wp(\mathbf{t} := \mathbf{t} * (\mathbf{x} - 1); \mathbf{n} := \mathbf{n}/\mathbf{x}, wp(\text{Loop2}, P_0))) \vee (x \not\mid n \wedge P_0) \\
&\equiv (x \mid n \wedge wp(\mathbf{t} := \mathbf{t} * (\mathbf{x} - 1); \mathbf{n} := \mathbf{n}/\mathbf{x}, Q_0)) \vee Q_0 \\
&\equiv (x \mid n \wedge wp(\mathbf{t} := \mathbf{t} * (\mathbf{x} - 1), wp(\mathbf{n} := \mathbf{n}/\mathbf{x}, Q_0))) \vee Q_0 \\
&\equiv (x \mid n \wedge wp(\mathbf{t} := \mathbf{t} * (\mathbf{x} - 1), x \neq 1 \wedge \frac{n}{x} = 1 \wedge t = 1)) \vee Q_0 \\
&\equiv (x \mid n \wedge x \neq 1 \wedge \frac{n}{x} = 1 \wedge t(x - 1) = 1) \vee Q_0 \\
&\equiv (x = 2 \wedge n = 2 \wedge t = 1) \vee (x \neq 1 \wedge n = 1 \wedge t = 1)
\end{aligned}$$

We then apply the first assignment of *Body1*:

$$\begin{aligned}
wp(\text{Body1}, P_0) &\equiv wp(\mathbf{x} := \mathbf{x} + 1, wp(\text{Condit}, P_0)) \\
&\equiv (x = 1 \wedge n = 2 \wedge t = 1) \vee (n = 1 \wedge t = 1)
\end{aligned}$$

This allows us to define  $P_1$ :

$$\begin{aligned}
P_1 &\equiv n \neq 1 \wedge wp(\text{Body1}, P_0) \\
&\equiv x = 1 \wedge n = 2 \wedge t = 1
\end{aligned}$$

(iii)  $P_2$  for  $wp(\text{Loop1}, t = 1)$

Start with  $wp(\text{Loop2}, P_1)$ :

$$\begin{aligned}
R_0 &\equiv x \not\mid n \wedge P_1 \\
&\equiv x \not\mid n \wedge x = 1 \wedge n = 2 \wedge t = 1 \\
&\equiv \mathbf{False}
\end{aligned}$$

Therefore  $R_k \equiv \mathbf{False}$  for all  $k$  because the loop can never terminate with postcondition  $P_1$ .

$$\begin{aligned}
wp(\text{Loop2}, P_1) &\equiv \exists k. (k \geq 0 \wedge \mathbf{False}) \\
&\equiv \mathbf{False}
\end{aligned}$$

Hence

$$\begin{aligned}
wp(\text{Condit}, P_1) &\equiv (x \mid n \wedge wp(\mathbf{t} := \mathbf{t} * (\mathbf{x} - 1); \mathbf{n} := \mathbf{n}/\mathbf{x}, \mathbf{False})) \vee (x \not\mid n \wedge P_1) \\
&\equiv \mathbf{False} \vee \mathbf{False} \quad (\text{because } wp(S, \mathbf{False}) = \mathbf{False} \text{ always}) \\
&\equiv \mathbf{False}
\end{aligned}$$

And therefore

$$\begin{aligned}
wp(\text{Body1}, P_1) &\equiv wp(\mathbf{x} := \mathbf{x} + 1, \mathbf{False}) \\
&\equiv \mathbf{False}
\end{aligned}$$

And finally:

$$\begin{aligned}
P_2 &\equiv n \neq 1 \wedge \mathbf{False} \\
&\equiv \mathbf{False}
\end{aligned}$$

(iv)  $P_k$  for  $wp(\text{Loop1}, t = 1)$  and  $k > 2$

$P_k \equiv \mathbf{False}$  for  $k \geq 2$  because if a loop cannot terminate with a given postcondition after 2 steps then it cannot terminate after any larger number of steps.

(v)  $wp(\text{Totient}, t = 1)$

$$\begin{aligned} wp(\text{Loop1}, t = 1) &\equiv \exists k. (k \geq 0 \wedge P_k) \\ &\equiv (n = 1 \wedge t = 1) \vee (x = 1 \wedge n = 2 \wedge t = 1) \vee \mathbf{False} \vee \mathbf{False} \vee \dots \\ &\equiv (n = 1 \wedge t = 1) \vee (x = 1 \wedge n = 2 \wedge t = 1) \end{aligned}$$

And finally

$$\begin{aligned} wp(\text{Totient}, t = 1) &\equiv wp(\mathfrak{t} := 1; \mathfrak{x} := 1, wp(\text{Loop1}, t = 1)) \\ &\equiv wp(\mathfrak{t} := 1, wp(\mathfrak{x} := 1, wp(\text{Loop1}, t = 1))) \\ &\equiv wp(\mathfrak{t} := 1, (n = 1 \wedge t = 1) \vee (1 = 1 \wedge n = 2 \wedge t = 1)) \\ &\equiv (n = 1 \wedge 1 = 1) \vee (1 = 1 \wedge n = 2 \wedge 1 = 1) \\ &\equiv n = 1 \vee n = 2 \end{aligned}$$