Problem Set 6
Safe and Secure Software (WS 11/12)

Bauhaus-University Weimar, Chair of Media Security
Prof. Dr. Stefan Lucks, Christian Forler
Url: `http://www.uni-weimar.de/cms/medien/mediensicherheit`

Problem 1: Hoare Logic (4 Points)
Show the total correctness for the following code.

```
procedure Trine_Sort(A : Array; X,Y,Z : Natural) is
  if A(Y) > A(Z) then
     T := A(Y);
     A(Y) := A(Z);
     A(Z) := T;
  if A(X) > A(Y) then
     T := A(Y);
     A(Y) := A(X);
     A(X) := T;
  if A(Y) > A(Z) then
     T := A(Y);
     A(Y) := A(Z);
     A(Z) := T;
end Trine_Sort;
{A(X)<=A(Y), A(Y)<=A(Z)}
```

Mini-Project 1 (4 Points)

a) Read Chapter 8 of JE, and solve Exercises 8.1-8.4.

b) Write a `testgen` "test driver" for your solution.

Mini-Project 2 (4 Points)

a) Read Chapter 11 of JE, and solve Exercises 11.1 and 11.3.

b) Write a `testgen` "test driver" for your solution.

Mini-Project 3 (4 Points)

a) Implement a subprogram (function or procedure) in Ada, that computes the *greatest common divisor*.

b) Show the total correctness of your program using the Hoare logic.

c) Enrich your subprogram with the pre and postcondition (either Ada'12 or SPARK annotations) you have calculated from b).

Merry Christmas and Happy New Year!