Dr. Matthias Heizmann
Dominik Klumpp

Hand in until 16:00 on May 12, 2021
Discussion: May 12, 2021

# Tutorial for Program Verification
## Exercise Sheet 6

In this exercise we work with the programming & verification language Boogie.

Submit your solution by uploading your programs as text files on ILIAS.

**Exercise 1: Boogie** 2 Points

Using the Boogie[1] language, implement the following programs:

(a) Implement a procedure with the signature `gcd(x : int, y : int) returns (z : int)` that takes two (mathematical) integers $x, y$ and, if they are both not equal to 0, computes their greatest common divisor $z$. The algorithm may only make use of addition and subtraction, but not use multiplication, division or modulo.[2]

(b) Implement a procedure with the signature `pow(x : int, y : int) returns (exp : int)` that takes two integers $x, y$, and, if $y$ is greater than 0, returns $x^y$.

You can use the Boogie interpreter Boogaloo[3] to test your program. A user manual is available online[4].

[1] `https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/krml178.pdf`
[2] Hint: `https://en.wikipedia.org/wiki/Euclidean_algorithm`
[3] `http://comcom.csail.mit.edu/comcom/#Boogaloo`
[4] `https://github.com/nadia-polikarpova/boogaloo/wiki/User-Manual`