apl. Prof. Dr. Thomas Noll
Kevin van der Pol, Hao Wu

Exercise 1 (Assertions): (1+1 Points)

a) Give an assertion $A \in Assn$ with logical variables $i, j, k \in LVar$, expressing that k is the greatest common divisor of i and j, i.e. $k = gcd(i, j)$.

b) Goldbach's conjecture states that every even $n \in \mathbb{N}$ can be expressed as the sum of two primes p_1 and p_2. Such a pair of primes is called a *Goldbach partition* of n. Give the partial correctness property of a program P that computes the Goldbach partition of any given even natural number.

Why would the existence of such a program P, i.e. a program that satisfies this partial correctness property, not prove Goldbach's conjecture?

Exercise 2 (Greatest Common Divisor): (3+4 Points)

a) Show that the *greatest common divisor* of two positive integers $i, j \in \mathbb{Z}$, denoted by $\text{gcd}(i, j)$, has the following properties:

a) $i > j \Rightarrow \text{gcd}(i, j) = \text{gcd}(i - j, j)$,

b) $\text{gcd}(i, j) = \text{gcd}(j, i)$, and

c) $\text{gcd}(i, i) = i$.

b) Using the Hoare rules, prove that the statement $c \in \textbf{Cmd}$ given by

$$\textbf{while } \neg(x = y) \textbf{ do if } x \leq y \textbf{ then } y := y - x \textbf{ else } x := x - y,$$

satisfies the following partial correctness property:

$$\{x = i \wedge y = j \wedge i \geq 1 \wedge j \geq 1\}\ c\ \{x = \text{gcd}(x, y) = \text{gcd}(i, j)\}.$$

Exercise 3 (Repeat ... Until): (1+3 Points)

a) Develop a proof rule for statements of the form **repeat** c **until** b where $c \in \textbf{Cmd}$ and $b \in \textbf{BExp}$ (without assuming the presence of a **while** statement in the programming language).

b) Using this rule (and the known proof system), establish the validity of the following partial correctness property:

$$\{y \geq 0\} z := 0; x := 0;\ \textbf{repeat } z := z + x; x := x + 1 \textbf{ until } x > y \left\{z = \frac{y(y+1)}{2}\right\}$$