Assignment on Hoare Logic

1. Fill in the missing precedents indicated by question marks to make the following specifications true. The assertions that you provide should be as weak as possible, but they should not be unnecessarily complicated.

$$[?]\ x := x + 1; y := y + 2 * x - 1;\ [y = x^2]$$
$$[?]\ x := x + y; y := x - y; x := x - y;\ [x = z \wedge y = w]$$
$$[?]\ \textbf{while}\ a < b\ \textbf{do}\ (a := a + 1; y := x + y;)\ [y = x * b]$$
$$[?]\ \textbf{while true do skip}\ [\textbf{false}]$$
$$\{?\}\ \textbf{while true do skip}\ \{\textbf{false}\}$$

2. (Taken from the course exam in Autumn 2019)

   Give a formal proof, using the Hoare logic rules, of the following partial-correctness specification.

$$\{x = 0\}$$
$$\textbf{while}\ x < 100\ \textbf{do}\ (x := x + 1; y := x;)$$
$$\{x = 100 \wedge y = 100\}$$

   Also, write down the loop invariant in your proof.

3. (Taken from the course exam in Autumn 2018)

   (a) Consider Hoare triples of the form $\{\textbf{true}\}x := e\{x = e\}$.

      i. Write down an instance of such a triple that cannot be proved using Hoare logic and explain why not.

      ii. Write down conditions on x and e such that $\{\textbf{true}\}x := e\{x = e\}$ can be proved and give a proof of this assuming your conditions.

   (b) Consider Hoare triples of the form $[\textbf{true}]c[\textbf{true}]$. Write down an instance of such a triple that cannot be proved using Hoare logic and explain why not.

4. (Taken from the course exam in Autumn 2018)

   In this problem we add the "repeat" command to the simple imperative language. We extend the syntax as follows:

$$(\mathit{Comm})\quad c\quad ::=\quad \ldots \mid \textbf{repeat}\ c\ \textbf{until}\ b$$

The meaning of **repeat** c **until** b is that c is executed and then b is tested; if the result is **true**, then nothing more is done, otherwise the whole **repeat** command is repeated. Thus **repeat** c **until** b is equivalent to c **; while** $\neg b$ **do** c.

Give the partial correctness Hoare logic rule for **repeat** c **until** b.