

**Semantyka i weryfikacja programów 2023/24.**  
**Zadanie domowe 3.**

Na kolejnej stronie podany jest program zapisany w języku TINY rozszerzonym o operację `_ div2` dzielenia całkowitego przez 2 oraz, na potrzeby formułowania asercji, o operację podnoszenia liczb całkowitych do całkowitej nieujemnej potęgi. Jak widać z podanej specyfikacji, jest to kolejna wersja liczenia pierwiastka całkowitego liczby całkowitej dodatniej.

Udowodnij częściową poprawność tego programu względem podanej specyfikacji, podając niezmienniki obu pętli oraz wstawiając odpowiednie formuły w nawiasy `{...}` tak, aby podane niezmienniki i asercje zapisały przeprowadzony dowód częściowej poprawności programu w logice Hoare'a. Jeśli w dwóch sąsiednich wierszach występują nawiasy `{...}` to pomiędzy wstawionymi tam asercjami powinna zachodzić implikacja. Można też dodać dodatkowe nawiasy i wpisać w nie odpowiednie asercje. Poza niezmiennikami  $\gamma_1$  i  $\gamma_2$ , wymagane jest przynajmniej podanie formuł  $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$  (ale ewentualne błędy w innych formułach też będą wpływały na ostateczną ocenę rozwiązania).

**Wskazówka:**

$$(r + i)^2 = (r + 2 * i)^2 - 2 * r * i - 3 * i^2$$

**Uwaga:** Do sformatowania rozwiązania w wersji elektronicznej można wykorzystać dostępne na stronie wykładu pliki:

- `zad3dom2023program.txt` — tekst programu
- `zad3dom2023program.tex` — plik L<sup>A</sup>T<sub>E</sub>X'a z programem i miejscem na wpisanie niezmienników i asercji.

```

{ n > 0 }
i := 1;
{
kw := 4;
{
while { $\gamma_1$ :
    kw  $\leq$  n
do
    (
    {
    i := 2*i;
    { $\alpha_1$ :
    kw := 4*kw
    {
    )
{ $\alpha_2$ :
r := i;
{
dri := kw div2;
{
ik := dri div2;
{
while { $\gamma_2$ :
    i > 1
do
    (
    {
    i := i div2;
    { $\alpha_3$ :
    ik := (ik div2) div2;
    {
    dri := dri div2;
    { $\alpha_4$ :
    if (kw - dri - 3*ik)  $\leq$  n
    then
        {
        r := r + i;
        { $\alpha_5$ :
        dri := dri + 2*ik
        {
    else
        {
        kw := kw - dri - 3*ik;
        {
    )
{
{  $r^2 \leq n < (r + 1)^2$  }

```