Séance d'exercices 9°

Preuve de programme

25 mai 2004

En groupes de deux, prouvez que le programme

```
const int x, n;
int y;
{
  int i, z;
  i := n;
  y := 1;
  z := x;
  while (i > 0)
  {
    while (i%2 = 0)
    {
      z := z · z;
      i := i/2;
    }
    y := y · z;
    i--;
  }
}
```

calcule bien la $n$ième puissance du nombre entier x pour tout $n \geq 0$. ($\%$ est un symbole fonctionnel binaire qui désigne l'opération calculant le reste entier d'une division.)

Dans ce but, prouvez formellement — moyennant la logique de Hoare — que y est égale à cette puissance *si le programme termine*, et ensuite prouvez informellement que le programme termine effectivement. Inspirez-vous de l'étude de cas 4° et utilisez le fait (théorème) que si $i > 0$ est pair alors $\mathrm{p}(z, i) = \mathrm{p}(\mathrm{p}(z, 2), i/2) = \mathrm{p}(z \cdot z, i/2)$ où p désigne la fonction puissance.