Travaux dirigés et pratiques
Racine carrée entière (TD 10)

Sylvain Chevillard et Damien Pous

12 mai 2008

Ces exercices doivent être faits en ayant chargé les bibliothèques suivantes :

```
Require Export ZArith.
Require Export Omega.
Require Export ZArithRing.
Open Scope Z_scope.
```

1 Rappel sur Z.

On rappelle que les nombres positifs sont représentés dans la bibliothèque `ZArith` par le type suivant :

```
Inductive positive  : Set :=
         xI : positive->positive
       | xO : positive->positive
       | xH : positive.
```

Le constructeur `xH` doit être interprété comme la constante 1, le constructeur `xO` doit être interprété comme la fonction $\lambda x.\ 2x$ et le constructeur `xI` doit être interprété comme la fonction $\lambda x.\ 2x + 1$.

Le type des entiers relatifs est construit à partir du type des nombres positifs par la définition inductive suivante :

```
Inductive Z  : Set :=
       ZERO : Z
      | POS : positive->Z
      | NEG : positive->Z.
```

2 Analyse du problème.

Etant donné un nombre positif (strictement, c'est plus simple) `p`, on veut calculer une paire de nombres `s` et `r` tels que

$$s^2 \leqslant p < (s+1)^2 \quad \text{et} \quad p = s^2 + r.$$

On adopte un algorithme de calcul adapté à la représentation binaire des entiers de `Z`. Posons $p = 4q + r_0$ avec $r_0 < 4$. Si `s'` et `r'` sont les résultats du calcul de la racine carrée de `q`, alors il existe deux possibilités :

1. `Si 4*r'+r0 < 4*s'+1 alors s=2s' et r=4*r'+r0`
2. `sinon s=2*s'+1 et r=4*r'+r0-4*s'-1`

On va donc construire une fonction qui calcule la racine carrée en utilisant cet algorithme, et qui est donc basée sur une récurrence structurelle sur `p` dans laquelle un pas correspond à une division par quatre. Cette fonction aura le type suivant :

```
forall p:positive,
  {s:Z &{r:Z | Zpos p = s*s+r /\ s*s <= Zpos p < (s+1)*(s+1)}}
```

Indications :
- La division par 4 est obtenue par un simple filtrage sur la structure des nombres positifs.
- La comparaison de deux nombres entiers pourra être faite avec la fonction `Z_lt_ge_dec`.
- Les égalités se démontreront facilement avec la tactique `ring`.
- Les comparaisons poseront plus de problèmes à cause de l'apparition de carrés de variables mais vous devriez quand même faire apparaitre des formules susceptibles d'être traitées par `omega`.
- On suggère de travailler en trois temps.

3 Pour se mettre en jambes.

On pourra choisir pour l'essentiel du travail une spécification équivalente à celle de l'énoncé mais ayant des inégalités linéaires et non quadratiques de façon à pouvoir utiliser la tactique `omega`.
Pour débuter la récurrence, on va avoir besoin de trois théorèmes démontrant la correction de la spécification de la racine carrée de respectivement `1`, `2` et `3`.

4 Le cœur du travail.

Ecrire le squelette de la fonction calculant par récurrence modulo 4 la racine carrée de `p` pour tout `p` de type `positive`.
Outre les preuves de correction des cas de bases démontrés à la question précédente, on va avoir besoin des preuves de correction des pas de récurrence. Afin de sérier les problèmes, on propose de les mettre en hypothèses ou de les admettre ainsi :

```
Lemma ...
Proof.
Admitted.
```

Le but est de parvenir une écriture de la fonction syntaxiquement correcte.

5 Pour terminer.

Prouver chacun des lemmes admis précédemment. Si la spécification utilisée dans la fonction était différente de celle de l'énoncé, définir une racine carrée conforme à l'énoncé.