

Computing and Software 734
Formalized Mathematics
Winter 2008

Exercise 4

20 pts.

Due 5 March 2008

Assigned: 4 February 2008

Revised: 7 march 2008

Do this exercise with your group partner.

Formalize in your chosen theorem proving system the following definitions, lemmas, and proofs (written by Henk Barendregt):

Let \mathbf{N} be the set of natural numbers and P be the predicate on \mathbf{N} defined by

$$\forall m : \mathbf{N} . P(m) \equiv \exists n : \mathbf{N} . 0 < m \wedge m^2 = 2n^2.$$

Lemma 1 $\forall m : \mathbf{N} . P(m) \supset \exists m' : \mathbf{N} . (m' < m \wedge P(m')).$

Proof Indeed suppose $0 < m$ and $m^2 = 2n^2$. It follows that m^2 is even, but then m must be even, as odds square to odds. So $m = 2k$ and we have $2n^2 = m^2 = 4k^2$ which implies $n^2 = 2k^2$. Since $0 < m$, it follows that $0 < m^2$, $0 < n^2$, and $0 < n$. Therefore $P(n)$ holds. Moreover, $n^2 < n^2 + n^2 = m^2$, so $n^2 < m^2$ and hence $n < m$. So we can take $m' = n$. \square

Lemma 2 $\forall m, n : \mathbf{N} . m^2 = 2n^2 \supset m = n = 0.$

Proof By Lemma 1, $\forall m : \mathbf{N} . \neg P(m)$, since there are no infinite descending sequences of natural numbers. Now suppose $m^2 = 2n^2$ with $m \neq 0$. Then $0 < m$ and hence $P(m)$, which is a contradiction. Therefore, $m = 0$. But then also $n = 0$. \square

Send the instructor the files you produced with comments and instructions on how they can be loaded and checked.