$\neg\sqrt{2} \in \mathbb{Q}$

—

3 Proofs in ProofPower-HOL

R.D. Arthan
Lemma 1 Ltd.
rda@lemma-one.com

20th March 2005*

Some while ago Freek Wiedijk proposed the irrationality of $\sqrt{2}$ as an interesting example to use in a comparative study of different proof assistants. Freek received formalisations using many systems and has prepared a report presenting the results. He was recently kind enough to draw my attention to a draft of his very interesting introduction to the report. This kind thought led to a small flurry of comments and then to the present contribution to the study using the ProofPower system. My apologies to Freek for creating extra work at the last minute.

The formal material is based on the mathematical case studies in ProofPower-HOL that have been under evolutionary development over the last few years. The present (March 2005) version of this document does not yet form part of the official case studies, but parts of it are likely to be included in them when one or two obvious gaps in the breadth of coverage have been filled (most conspicuously the fundamental theorem of arithmetic). This note follows the mathematical case studies in including theory listings for all the theories developed (in sections 6 to 10). We use a slightly different approach in the discussion (giving the statements of the main results as ML quotations).

In retrospect, one of my main comments on Freek's report amounted to my surprise that the theorem-proving community only seemed to know one proof! The irrationality of $\sqrt{2}$ has several proofs and so, in the interests of variety, three proofs are presented here. Proof 1 is an ancient, but seemingly not so widely known, "geometrical" proof that requires no number theory. This proof is amenable to some interesting generalisations, but we do not look into that here (see, for example, *The Book of Numbers* by John H. Conway and Richard K. Guy). Proof 2 and proof 3 are the well-known proofs based on divisibility. Perhaps the least well-known thing about the well-known proofs is that there are two of them! We present them in reasonably full generality (showing in one case that the square root of any prime number is irrational, and in the other, that, if the square root of an integer is rational than the square root is actually an integer). Following Freek's rules, we are careful to derive the specific conclusion that $\sqrt{2}$ is irrational from the general proofs.

*Revised 11th November 2013 to be compatible with the latest version of the ProofPower mathemical case studies.

1 Common Definitions

The problem clearly needs to be formalised in terms of the 5 symbols forming the title of this document. Of these, logical negation, the number 2 and the membership sign are supplied for free. The square root function is defined in the theory of analysis from the mathematical case studies with the following defining property:

$$\vdash \forall\, x \bullet\ 0. \leq x \Rightarrow 0. \leq Sqrt\ x \wedge Sqrt\ x \hat{}\ 2 = x$$

The proofs use no facts of analysis other than this definition. We need to define the set of rational numbers. The definition is common to all three proofs: after all, we want the three proofs all to prove exactly the same thing.

The following red tape sets up a theory *sqrt_defs* to hold this material.

SML

```
set_pc "basic_hol1";
open_theory "analysis";
force_delete_theory "sqrt2_defs" handle Fail _ => ();
new_theory "sqrt2_defs";
```

To state what is proved by the third proof, we need the set of integers as well as the set of rationals. The definitions follow (in the usual ProofPower-HOL constant specification boxes where we give the signature of the new constant and its desired defining property separated by a horizontal bar). The consistency of these equational definitions is proved automatically.

HOL Constant

$$\mathbb{Z} : \mathbb{R}\ SET$$

$$\mathbb{Z} = \{x \mid \exists m : \mathbb{N} \bullet x = \mathbb{NR}\ m \vee x = \sim(\mathbb{NR}\ m)\}$$

Here $\mathbb{NR}$ is the function that injects the type of natural numbers into the type of reals.

HOL Constant

$$\mathbb{Q} : \mathbb{R}\ SET$$

$$\mathbb{Q} = \{x \mid \exists a\ b : \mathbb{N} \bullet \neg b = 0 \wedge (x = a/b \vee x = \sim(a/b))\}$$

A handful of basic theorems about the square root function are developed in this theory, see the listing for details.

2 Proof 1

Our first proof is very simple. It makes no reference to prime divisors or the like. It is inspired by the construction depicted in figure 1. If we let $x = BD$ and $y = AB$ be respectively the diagonal and side of the larger square, so that $x/y = \sqrt{2}$, $DE = 2y - x$ and $DF = x - y$ form the diagonal and side of the smaller square. But then, if x and y were both integers, so also would be $x - y$ and $2y - x$ and we would have a contradiction, since we could repeat the construction to produce arbitrarily small squares with integer sides.

This proof translates very simply into algebra. To present the formalisation, we give the statements of a selection of the lemmas proved. The theory listings towards the end of the document give the output from ProofPower showing that these results have indeed been proved. The actual proof scripts are included in the master source text of this document, but not in the printed form.

The main work in this proof is given in a series of 5 lemmas. The first lemma gives the key algebraic facts about the geometrical construction. It also includes what amounts to the estimate that $1 < \sqrt{2} < 3/2$, which is needed to show that when the inputs to the construction are positive integers, then so are the outputs.

SML

$$
\begin{array}{l}
val\ \mathbf{proof1\_lemma1} = \ulcorner \\
\forall x\ y \bullet \\
\quad \mathbb{NR}\ 0 \leq x \wedge \mathbb{NR}\ 0 < y \wedge x \hat{}\ 2 = \mathbb{NR}\ 2 * y \hat{}\ 2 \\
\Rightarrow \quad y < x \wedge \mathbb{NR}\ 2 * x \leq \mathbb{NR}\ 3 * y \\
\wedge \quad (\mathbb{NR}\ 2 * y - x) \hat{}\ 2 = \mathbb{NR}\ 2 * (x - y) \hat{}\ 2 \\
\urcorner;
\end{array}
$$

The second and third lemmas (see the theory listing in section 7) essentially just specialise the above to the case where x and y are natural numbers.

All three proofs proceed by Fermat's "method of infinite descent". I.e., one shows that the existence of a positive integer counter-example to a conjecture implies the existence of a smaller counter-example. Thus in each case we have an "inductive step" that produces smaller counter-examples from larger ones. The following lemma gives this step for the present proof:

SML

$$
\begin{array}{l}
val\ \mathbf{proof1\_lemma4} = \ulcorner \\
\forall m\ n \bullet \\
\quad \mathbb{NR}\ m \hat{}\ 2 = \mathbb{NR}\ 2 * \mathbb{NR}\ n \hat{}\ 2 \wedge 0 < n \\
\Rightarrow \quad \exists m1\ n1 \bullet 0 < n1 \wedge n1 < n \wedge \mathbb{NR}\ m1 \hat{}\ 2 = \mathbb{NR}\ 2 * \mathbb{NR}\ n1 \hat{}\ 2 \\
\urcorner;
\end{array}
$$

From this we conclude that the only natural number solution to $m^2 = 2n^2$ has $n = 0$.

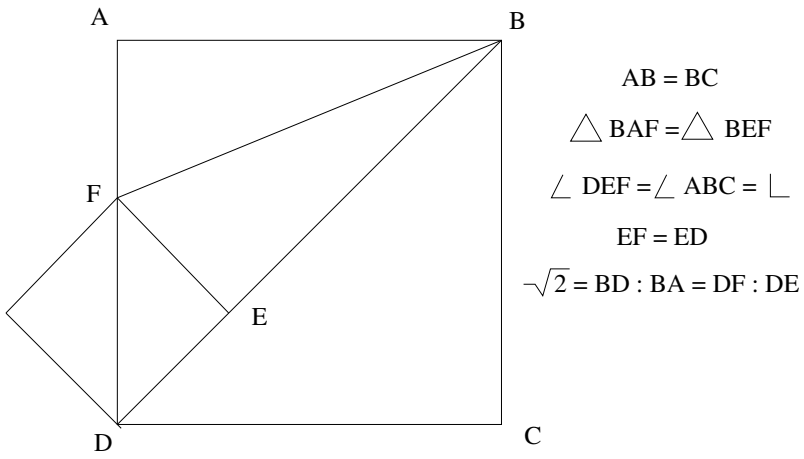

Figure 1: The Geometrical Construction

SML
```
val proof1_lemma5 = ⌜
        ∀n m• ℕℝ m ^ 2 = ℕℝ 2 * ℕℝ n ^ 2 ⇒ n = 0
⌝;
```

The desired result follows easily from the above. We formalise it in two guises, the first guise is explicit:

SML
```
val proof1_thm1 = ⌜
        ∀a b• ¬b = 0 ⇒ ¬(a/b)^2 = ℕℝ 2
⌝;
```

The second guise gives the result much as it is stated in the title of this note:

SML
```
val proof1_thm2 = ⌜
        ¬Sqrt (ℕℝ 2) ∈ ℚ
⌝;
```

3 Divisibility

The other two proofs we give are the better known ones based on divisibility. They share common material from the theory of divisibility. In this section we define the common notions. First we set up a theory to hold the definitions. See section 8 for the listing of this theory.

SML
```
open_theory "fin_set";
force_delete_theory "divisibility" handle Fail _ => ();
new_theory "divisibility";
```

We have a choice about whether to develop the theory for the natural numbers or for the integers. On the one hand, it is more pleasant to work in a ring rather than a semi-ring, on the other hand negative numbers are not very relevant to the main results, even when they are useful in the proofs. We vote in favour of the natural numbers, and proceed to define the greatest common divisor function. This is an implicit definition: the first of the two conjuncts in the defining property say that the greatest common divisor is a common divisor and the second says that it is the greatest one (i.e., it is maximal with respect to the divisibility ordering of the natural numbers). We have several choices about how to capture formally the notion *"m is divisible by n"*. We opt to state it as $m\ Mod\ n = 0$.

HOL Constant

$$\boldsymbol{Gcd} : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$$

$$\begin{array}{lll}
(\forall m\ n\bullet & & 0 < m \wedge 0 < n \\
\quad \Rightarrow & & 0 < Gcd\ m\ n \\
\quad \wedge & & m\ Mod\ Gcd\ m\ n = 0 \\
\quad \wedge & & n\ Mod\ Gcd\ m\ n = 0) \\
\wedge\ (\forall m\ n\ d\bullet & & 0 < d \\
\quad \wedge & & m\ Mod\ d = 0 \\
\quad \wedge & & n\ Mod\ d = 0 \\
\quad \Rightarrow & & Gcd\ m\ n\ Mod\ d = 0)
\end{array}$$

Now we define the set of prime numbers:

HOL Constant

$$\boldsymbol{Prime} : \mathbb{N}\ SET$$

$$Prime = \{p \mid 1 < p \wedge \forall m\ n\bullet\ p = m{*}n \Rightarrow m = 1 \vee n = 1\}$$

The important fact we need about prime numbers is the fact that a number is prime iff. it is greater than 1 and whenever it divides a product it divides one of the factors. The right-to-left direction of this is simple. It is for this the other direction that we need to develop the theory of the g.c.d.

SML

$$\begin{array}{lll}
val\ \boldsymbol{prime_thm} = \ulcorner & & \\
\quad \forall p\bullet & & p \in Prime \\
\quad \Leftrightarrow & & 1 < p \\
\wedge & & (\forall m\ n\bullet\ (m{*}n)\ Mod\ p = 0 \Rightarrow m\ Mod\ p = 0 \vee n\ Mod\ p = 0) \\
\urcorner; & &
\end{array}$$

The bulk of the theory then comprises the supporting lemmas and theorems we need to prove that the definition of greatest common divisor is consistent and to reason about it (see the theory listing in section 8 for full details). The most common textbook account exhibits the g.c.d. of m and n as the smallest positive value of the form $am+bn$. This requires a and b to range over negative integers. A slightly less symmetrical alternative is to take the g.c.d. to be the smallest positive value of the form $(am)\ Mod\ n$. This works over the natural numbers. The main result (after the consistency theorem) is the following:

SML

$$\begin{array}{lll}
val\ \boldsymbol{gcd_eq_mod_thm} = \ulcorner & & \\
\quad \forall m\ n\bullet & & 0 < m \wedge 0 < n \wedge 0 < m\ Mod\ n \\
\quad \Rightarrow & & \exists a\bullet\ 0 < (a{*}m)\ Mod\ n \\
\quad \wedge & & (\forall b\bullet\ 0 < (b{*}m)\ Mod\ n \Rightarrow (a{*}m)\ Mod\ n \leq (b{*}m)\ Mod\ n) \\
\quad \wedge & & Gcd\ m\ n = (a{*}m)\ Mod\ n \\
\urcorner; & &
\end{array}$$

The final theorem in this theory for the current version of this document says that any integer greater than 1 has a prime divisor.

SML

```
val prime_divisor_thm = ⌜
        ∀m• 1 < m ⇒ ∃p n•p ∈ Prime ∧ m = p*n
⌝;
```

From this, it is a very short step to the fundamental theorem of arithmetic, but that is not needed for present purposes.

4 Proof 2

Our second proof is the most widely-known one: if $m^2 = 2n^2$, then m is even, but then so is n, so we can divide m and n by 2 to get a solution with smaller n. This gives a contradiction, because if there is a solution for n positive, we get an infinite descending sequence of positive integers. This proof generalises to show that $\sqrt{p}$ is irrational for any prime p.

To quote the formal steps in the proof we need to construct a theory in which the common definitions and the material on divisibility is available. The lemmas and theorems making up the proof are later stored in this theory. See section 9 for the listing.

SML

```
open_theory "divisibility";
force_delete_theory "sqrt2_proof2" handle Fail _ => ();
new_theory "sqrt2_proof2";
new_parent"sqrt2_defs";
```

The proof starts with the following lemma, the proof of which is easy given the results on divisibility. This is almost identical to lemma 4 in the 1st proof, but with an arbitrary prime p in place of the specific number 2. Of course, the method of proof is quite different: one observes that under the stated conditions, p must divide both m and n and so dividing through by it gives a smaller solution.

SML

```
val proof2_lemma1 = ⌜
∀p m n•                p ∈ Prime ∧ m * m = p * n * n ∧ 0 < n
⇒       ∃m1 n1•0 < n1 ∧ n1 < n ∧ m1 * m1 = p * n1 * n1
⌝;
```

From this it follows that the only solution to $m^2 = pn^2$ in natural numbers m and n has $n = m = 0$. Whence:

SML

```
val proof2_thm2 = ⌜
        ∀p•p ∈ Prime ⇒ ¬Sqrt (ℕℝ p) ∈ ℚ
⌝;
```

Freek quite rightly insists that we actually prove that $\sqrt{2}$ is irrational, so we need to prove that it is prime.

SML

```
val proof2_lemma3 = ⌜
        2 ∈ Prime
⌝;
```

Whence we draw the usual conclusion:

```
SML
val proof2_thm3 = ⌜
        ¬Sqrt (ℕℝ 2) ∈ ℚ
⌝;
```

5 Proof 3

This is the most general of the three proofs we give: if $m^2 = kn^2$ for any natural numbers k, m and n with k positive and $n > 1$, then any prime divisor of n is also a prime divisor of m. Thus by the usual infinite descent the only solutions of this equation with k and n positive have $n = 1$, i.e., the only solutions are when $k = m^2$ is a square.

As in the previous section we need to create a theory in which the right vocabulary is available to state the results: The lemmas and theorems making up the proof are later stored in this theory. See section 10 for the listing.

```
SML
open_theory "divisibility";
force_delete_theory "sqrt2_proof3" handle Fail _ => ();
new_theory "sqrt2_proof3";
new_parent"sqrt2_defs";
```

The first lemma is the following. It justifies the steps in the infinite descent.

```
SML
val proof3_lemma1 = ⌜
∀k m n•       0 < k ∧ m * m = k * n * n ∧ 1 < n
⇒       ∃m1 n1•0 < n1 ∧ n1 < n ∧ m1 * m1 = k * n1 * n1
⌝;
```

The next step is rather different. The infinite descent bottoms out at 1, from which we we conclude that if $m^2 = kn^2$ has a natural number solution with n positive, then k is a perfect square.

```
SML
val proof3_lemma2 = ⌜
∀k n m•       ℕℝ 0 < ℕℝ k ∧ ℕℝ 0 < ℕℝ n ∧ ℕℝ m ^ 2 = ℕℝ k * (ℕℝ n ^ 2)
⇒       ∃i• ℕℝ i ^ 2 = ℕℝ k
⌝;
```

With intermediate steps similar to the previous proofs, we arrive at the following:

```
SML
val proof3_thm2 = ⌜
∀i• ℕℝ 0 ≤ i ∧ i ∈ ℤ ∧ Sqrt i ∈ ℚ ⇒ Sqrt i ∈ ℤ
⌝;
```

Yet again, we must exercise our skills on the specific number 2, which requires the following lemma (easily proved using the numerical estimate that $1 < \sqrt{2} < 2$).

SML
```
val proof3_lemma3 = ⌜
        ¬Sqrt (ℕℝ 2) ∈ ℤ
⌝;
```

From which we conclude for the third and final time our old friend:

SML
```
val proof3_thm3 = ⌜
        ¬Sqrt (ℕℝ 2) ∈ ℚ
⌝;
```

6 THE THEORY sqrt2_defs

6.1 Parents

analysis

6.2 Children

sqrt2_proof1 *sqrt2_proof3* *sqrt2_proof2*

6.3 Constants

$\mathbb{Z}$ $\mathbb{R}$ $\mathbb{P}$
$\mathbb{Q}$ $\mathbb{R}$ $\mathbb{P}$

6.4 Definitions

$\mathbb{Z}$ $\vdash \mathbb{Z} = \{x | \exists\ m \bullet\ x = \mathbb{NR}\ m \vee x = \sim (\mathbb{NR}\ m)\}$
$\mathbb{Q}$ $\vdash \mathbb{Q} = \{x | \exists\ a\ b \bullet \neg\ b = 0 \wedge (x = a\ /\ b \vee x = \sim (a\ /\ b))\}$

6.5 Theorems

sqrt_thm $\vdash \forall\ x \bullet\ 0. \leq x \Rightarrow Sqrt\ x\ \hat{}\ 2 = x$
square_even_thm
$\vdash \forall\ x \bullet \sim x\ \hat{}\ 2 = x\ \hat{}\ 2$
sqrt_eq_thm $\vdash \forall\ x\ y \bullet\ 0. \leq x \wedge x\ \hat{}\ 2 = y \Rightarrow x = Sqrt\ y$
sqrt_egs_thm $\vdash Sqrt\ 0. = 0.$
$\wedge\ Sqrt\ 1. = 1.$
$\wedge\ Sqrt\ 4. = 2.$
$\wedge\ Sqrt\ 9. = 3.$
square_square_root_mono_thm1
$\vdash \forall\ x\ y \bullet\ 0. \leq x \wedge 0. \leq y \Rightarrow (x\ \hat{}\ 2 < y\ \hat{}\ 2 \Leftrightarrow x < y)$
sqrt_less_thm
$\vdash \forall\ x\ y \bullet\ 0. \leq x \wedge 0. \leq y \Rightarrow (Sqrt\ x < Sqrt\ y \Leftrightarrow x < y)$

7 THE THEORY sqrt2_proof1

7.1 Parents

sqrt2_defs

7.2 Theorems

proof1_lemma1
$\vdash \forall\ x\ y$
$\bullet\ 0. \leq x \wedge 0. < y \wedge x \hat{}\ 2 = 2. * y \hat{}\ 2$
$\Rightarrow y < x$
$\wedge\ 2. * x \leq 3. * y$
$\wedge\ (2. * y - x) \hat{}\ 2 = 2. * (x - y) \hat{}\ 2$

proof1_lemma2
$\vdash \forall\ i\ j \bullet\ j \leq i \Rightarrow \mathbb{NR}\ (i - j) = \mathbb{NR}\ i - \mathbb{NR}\ j$

proof1_lemma3
$\vdash \forall\ m\ n$
$\bullet\ \mathbb{NR}\ m \hat{}\ 2 = 2. * \mathbb{NR}\ n \hat{}\ 2 \wedge 0 < n$
$\Rightarrow n < m$
$\wedge\ 2 * m \leq 3 * n$
$\wedge\ \mathbb{NR}\ (2 * n - m) \hat{}\ 2 = 2. * \mathbb{NR}\ (m - n) \hat{}\ 2$

proof1_lemma4
$\vdash \forall\ m\ n$
$\bullet\ \mathbb{NR}\ m \hat{}\ 2 = 2. * \mathbb{NR}\ n \hat{}\ 2 \wedge 0 < n$
$\Rightarrow (\exists\ m1\ n1$
$\bullet\ 0 < n1 \wedge n1 < n \wedge \mathbb{NR}\ m1 \hat{}\ 2 = 2. * \mathbb{NR}\ n1 \hat{}\ 2)$

proof1_lemma5
$\vdash \forall\ n\ m \bullet\ \mathbb{NR}\ m \hat{}\ 2 = 2. * \mathbb{NR}\ n \hat{}\ 2 \Rightarrow n = 0$

proof1_thm1 $\vdash \forall\ a\ b \bullet\ \neg\ b = 0 \Rightarrow \neg\ (a\ /\ b) \hat{}\ 2 = 2.$

proof1_thm1a $\vdash \forall\ a\ b$
$\bullet\ \neg\ b = 0 \Rightarrow \neg\ (a\ /\ b) \hat{}\ 2 = 2. \wedge \neg \sim (a\ /\ b) \hat{}\ 2 = 2.$

proof1_thm2 $\vdash \neg\ Sqrt\ 2. \in \mathbb{Q}$

8 THE THEORY divisibility

8.1 Parents

fin_set

8.2 Children

sqrt2_proof3 *sqrt2_proof2*

8.3 Constants

Gcd	$\mathbb{N} \to \mathbb{N} \to \mathbb{N}$
Prime	$\mathbb{N}\ \mathbb{P}$

8.4 Definitions

Gcd $\vdash$ *ConstSpec*
$(\lambda\ Gcd'$
$\bullet\ (\forall\ m\ n$
$\bullet\ 0 < m \wedge 0 < n$
$\Rightarrow\ 0 < Gcd'\ m\ n$
$\wedge\ m\ Mod\ Gcd'\ m\ n = 0$
$\wedge\ n\ Mod\ Gcd'\ m\ n = 0)$
$\wedge\ (\forall\ m\ n\ d$
$\bullet\ 0 < d \wedge m\ Mod\ d = 0 \wedge n\ Mod\ d = 0$
$\Rightarrow\ Gcd'\ m\ n\ Mod\ d = 0))$
Gcd

Prime $\vdash$ *Prime*
$= \{p | 1 < p \wedge (\forall\ m\ n \bullet\ p = m * n \Rightarrow m = 1 \vee n = 1)\}$

8.5 Theorems

min_∈_thm $\vdash \forall\ n\ a \bullet\ n \in a \Rightarrow Min\ a \in a$

min_≤_thm $\vdash \forall\ n\ a \bullet\ n \in a \Rightarrow Min\ a \leq n$

times_eq_0_thm
$\vdash \forall\ m\ n \bullet\ m * n = 0 \Rightarrow m = 0 \vee n = 0$

times_cancel_thm
$\vdash \forall\ k\ m\ n \bullet\ 0 < k \wedge k * m = k * n \Rightarrow m = n$

times_eq_eq_1_thm
$\vdash \forall\ m\ n \bullet\ 0 < n \wedge m * n = n \Rightarrow m = 1$

times_eq_1_thm
$\vdash \forall\ m\ n \bullet\ m * n = 1 \Rightarrow m = 1 \wedge n = 1$

div_mod_1_thm
$\vdash \forall\ m \bullet\ m\ Div\ 1 = m \wedge m\ Mod\ 1 = 0$

m_div_mod_m_thm
$\vdash \forall\ m \bullet\ 0 < m \Rightarrow m\ Div\ m = 1 \wedge m\ Mod\ m = 0$

zero_div_mod_thm
$\vdash \forall\ m \bullet\ 0 < m \Rightarrow 0\ Div\ m = 0 \wedge 0\ Mod\ m = 0$

less_div_mod_thm

$\vdash \forall\ m\ n \bullet\ n < m \Rightarrow n\ Div\ m = 0 \wedge n\ Mod\ m = n$

div_mod_times_cancel_thm

$\vdash \forall\ k\ m\ n$
$\bullet\ 0 < k$
$\Rightarrow (m * k + n)\ Div\ k = m + n\ Div\ k$
$\wedge (m * k + n)\ Mod\ k = n\ Mod\ k$

mod_clauses $\vdash \forall\ k\ m\ n$
$\bullet\ 0 < k$
$\Rightarrow (m * k)\ Mod\ k = 0$
$\wedge (k * m)\ Mod\ k = 0$
$\wedge (k * m + n)\ Mod\ k = n\ Mod\ k$
$\wedge (m * k + n)\ Mod\ k = n\ Mod\ k$
$\wedge (k + n)\ Mod\ k = n\ Mod\ k$
$\wedge (n + k)\ Mod\ k = n\ Mod\ k$
$\wedge 0\ Mod\ k = 0$
$\wedge k\ Mod\ k = 0$
$\wedge m\ Mod\ k\ Mod\ k = m\ Mod\ k$

mod_eq_0_thm $\vdash \forall\ m\ n \bullet\ 0 < n \Rightarrow (m\ Mod\ n = 0 \Leftrightarrow (\exists\ k \bullet\ m = k * n))$

mod_eq_0_mod_eq_0_thm

$\vdash \forall\ m\ n$
$\bullet\ 0 < m \wedge 0 < n \wedge m\ Mod\ n = 0 \wedge n\ Mod\ m = 0 \Rightarrow m = n$

mod_plus_homomorphism_thm

$\vdash \forall\ m\ n\ k$
$\bullet\ 0 < k \Rightarrow (m + n)\ Mod\ k = (m\ Mod\ k + n\ Mod\ k)\ Mod\ k$

mod_times_homomorphism_thm

$\vdash \forall\ m\ n\ k$
$\bullet\ 0 < k \Rightarrow (m * n)\ Mod\ k = (m\ Mod\ k * n\ Mod\ k)\ Mod\ k$

gcd_consistent_lemma1

$\vdash \forall\ m\ n$
$\bullet\ 0 < m \wedge 0 < n \wedge 0 < m\ Mod\ n$
$\Rightarrow (\exists\ a$
$\bullet\ 0 < (a * m)\ Mod\ n$
$\wedge (\forall\ b$
$\bullet\ 0 < (b * m)\ Mod\ n$
$\Rightarrow (a * m)\ Mod\ n \leq (b * m)\ Mod\ n))$

gcd_consistent_lemma2

$\vdash \forall\ m\ n\ a\ d$
$\bullet\ 0 < m \wedge 0 < n \wedge 0 < d \wedge m\ Mod\ d = 0 \wedge n\ Mod\ d = 0$
$\Rightarrow (a * m)\ Mod\ n\ Mod\ d = 0$

gcd_consistent_lemma3

$\vdash \forall\ a\ b\ m\ n\ p\ r\ s$
$\bullet\ a * m = b * (n + 1) + r \wedge m = p * r + s$
$\Rightarrow (\exists\ q \bullet\ (q * m)\ Mod\ (n + 1) = s\ Mod\ (n + 1))$

gcd_consistent_lemma4

$\vdash \forall\ a\ b\ m\ n\ p\ r\ s$
$\bullet\ a * m = b * (n + 1) + r \wedge n + 1 = p * r + s$
$\Rightarrow (\exists\ q \bullet\ (q * m)\ Mod\ (n + 1) = s\ Mod\ (n + 1))$

gcd_consistent_lemma5

$\vdash \forall\ m\ n\ k\ a$
$\bullet\ 0 < m$
$\wedge\ 0 < n$

$\wedge\ 0 < m\ Mod\ n$
$\wedge\ 0 < (a * m)\ Mod\ n$
$\wedge\ (\forall\ b$
$\bullet\ 0 < (b * m)\ Mod\ n$
$\Rightarrow (a * m)\ Mod\ n \leq (b * m)\ Mod\ n)$
$\Rightarrow m\ Mod\ ((a * m)\ Mod\ n) = 0$
$\wedge\ n\ Mod\ ((a * m)\ Mod\ n) = 0$

Gcd_consistent

$\vdash Consistent$
$(\lambda\ Gcd'$
$\bullet\ (\forall\ m\ n$
$\bullet\ 0 < m \wedge 0 < n$
$\Rightarrow 0 < Gcd'\ m\ n$
$\wedge\ m\ Mod\ Gcd'\ m\ n = 0$
$\wedge\ n\ Mod\ Gcd'\ m\ n = 0)$
$\wedge\ (\forall\ m\ n\ d$
$\bullet\ 0 < d \wedge m\ Mod\ d = 0 \wedge n\ Mod\ d = 0$
$\Rightarrow Gcd'\ m\ n\ Mod\ d = 0))$

gcd_eq_mod_thm

$\vdash \forall\ m\ n$
$\bullet\ 0 < m \wedge 0 < n \wedge 0 < m\ Mod\ n$
$\Rightarrow (\exists\ a$
$\bullet\ 0 < (a * m)\ Mod\ n$
$\wedge\ (\forall\ b$
$\bullet\ 0 < (b * m)\ Mod\ n$
$\Rightarrow (a * m)\ Mod\ n \leq (b * m)\ Mod\ n)$
$\wedge\ Gcd\ m\ n = (a * m)\ Mod\ n)$

prime_0_less_thm

$\vdash \forall\ p\bullet\ p \in Prime \Rightarrow 0 < p$

gcd_prime_thm

$\vdash \forall\ m\ p\bullet\ 0 < m \wedge p \in Prime \Rightarrow Gcd\ m\ p = 1 \vee Gcd\ m\ p = p$

prime_thm

$\vdash \forall\ p$
$\bullet\ p \in Prime$
$\Leftrightarrow 1 < p$
$\wedge\ (\forall\ m\ n$
$\bullet\ (m * n)\ Mod\ p = 0$
$\Rightarrow m\ Mod\ p = 0 \vee n\ Mod\ p = 0)$

prime_divisor_thm

$\vdash \forall\ m\bullet\ 1 < m \Rightarrow (\exists\ p\ n\bullet\ p \in Prime \wedge m = p * n)$

9 THE THEORY sqrt2_proof2

9.1 Parents

sqrt2_defs *divisibility*

9.2 Theorems

proof2_lemma1
$\vdash \forall\ p\ m\ n$
$\bullet\ p \in Prime \wedge m * m = p * n * n \wedge 0 < n$
$\Rightarrow (\exists\ m1\ n1$
$\bullet\ 0 < n1 \wedge n1 < n \wedge m1 * m1 = p * n1 * n1)$

proof2_lemma2
$\vdash \forall\ p\ n\ m$
$\bullet\ p \in Prime \wedge \mathbb{NR}\ m \hat{}\ 2 = \mathbb{NR}\ p * \mathbb{NR}\ n \hat{}\ 2 \Rightarrow n = 0$

proof2_thm1 $\vdash \forall\ p\ a\ b \bullet\ p \in Prime \wedge \neg\ b = 0 \Rightarrow \neg\ (a\ /\ b) \hat{}\ 2 = \mathbb{NR}\ p$

proof2_thm1a $\vdash \forall\ a\ b$
$\bullet\ p \in Prime \wedge \neg\ b = 0$
$\Rightarrow \neg\ (a\ /\ b) \hat{}\ 2 = \mathbb{NR}\ p \wedge \neg \sim (a\ /\ b) \hat{}\ 2 = \mathbb{NR}\ p$

proof1_thm2 $\vdash \forall\ p \bullet\ p \in Prime \Rightarrow \neg\ Sqrt\ (\mathbb{NR}\ p) \in \mathbb{Q}$

proof2_lemma3
$\vdash 2 \in Prime$

proof2_thm3 $\vdash \neg\ Sqrt\ 2. \in \mathbb{Q}$

10 THE THEORY sqrt2_proof3

10.1 Parents

sqrt2_defs *divisibility*

10.2 Theorems

proof3_lemma1
$\vdash \forall\ k\ m\ n$
$\bullet\ 0 < k \wedge m * m = k * n * n \wedge 1 < n$
$\Rightarrow (\exists\ m1\ n1$
$\bullet\ 0 < n1 \wedge n1 < n \wedge m1 * m1 = k * n1 * n1)$

proof3_lemma2
$\vdash \forall\ k\ n\ m$
$\bullet\ 0. < \mathbb{NR}\ k \wedge 0. < \mathbb{NR}\ n \wedge \mathbb{NR}\ m \hat{}\ 2 = \mathbb{NR}\ k * \mathbb{NR}\ n \hat{}\ 2$
$\Rightarrow (\exists\ i\bullet\ \mathbb{NR}\ i \hat{}\ 2 = \mathbb{NR}\ k)$

proof3_lemma3
$\vdash \neg\ Sqrt\ 2. \in \mathbb{Z}$

proof3_thm1 $\vdash \forall\ k\ a\ b$
$\bullet\ \neg\ b = 0 \wedge (a\ /\ b) \hat{}\ 2 = \mathbb{NR}\ k$
$\Rightarrow (\exists\ i\bullet\ \mathbb{NR}\ i \hat{}\ 2 = \mathbb{NR}\ k)$

proof3_thm2 $\vdash \forall\ i\bullet\ 0. \leq i \wedge i \in \mathbb{Z} \wedge Sqrt\ i \in \mathbb{Q} \Rightarrow Sqrt\ i \in \mathbb{Z}$

proof3_thm3 $\vdash \neg\ Sqrt\ 2. \in \mathbb{Q}$

Index