Mathematical Case Studies: Some Number Theory[*]

Rob Arthan
rda@lemma-one.com

31 December 2016

Abstract

This ProofPower-HOL document presents some definitions and theorems from number theory. The topics currently covered include: divisors and greatest common divisors; Euclid's algorithm; e infinitude of the primes; fundamental theorem of arithmetic; divergence of the series of prime reciprocals; Wilson's theorem.

Reference: LEMMA1/HOL/WRK074; Current git revision: b0522be

[*] First posted 19 December 2005; for full changes history see: https://github.com/RobArthan/pp-contrib.

Contents

1 INTRODUCTION

This document is one of a suite of mathematical case studies in ProofPower-HOL. It deals with some elementary number theory.

Topics currently covered include divisors and greatest common divisors, Euclid's algorithm, the infinitude of the primes, fundamental theorem of arithmetic, divergence of the series of reciprocals of the primes.

There are also a few definitions and lemmas relating to general subrings of the real numbers. These are used to define the subring of integers and the subfield of rational numbers.

2 THE THEORY *numbers*

2.1 Preliminaries

SML

```
force_delete_theory "numbers" handle Fail _ => ();
open_theory"fincomb";
new_theory "numbers";
set_merge_pcs["basic_hol1", "'sets_alg", "'ℤ", "'ℝ"];
```

2.2 Divisors in ℕ

We begin to develop the theory of divisors by first defining an infix relation, divides, such that *n* divides *m* iff. *m* is a multiple of *n*.

SML

```
declare_infix(200, "Divides");
```

HOL Constant

```
$Divides : ℕ → ℕ → BOOL
├──────────────────────────────
∀n m• n Divides m ⇔ ∃k• m = k * n
```

It is often convenient to reduce *n Divides m* to *m Mod n = 0*. The following block of theorems provide this and several other useful facts, e.g., that *Divides* is a partial ordering, i.e., it is reflexive, antisymmetric and transitive.

times_eq_0_thm
times_cancel_thm
times_eq_eq_1_thm
times_eq_1_thm
ℕ*_exp_clauses*
ℕ*_exp_eq_0_thm*
ℕ*_exp_eq_1_thm*
ℕ*_exp_1_thm*
ℕ*_exp_divides_thm*
ℕ*_exp_times_thm*
ℕ*_exp_*ℕ*_exp_thm*
div_mod_1_thm
m_div_mod_m_thm
zero_div_mod_thm
less_div_mod_thm
div_mod_times_cancel_thm
mod_clauses
div_clauses
mod_eq_0_thm
divides_0_thm
divides_trans_thm
divides_mod_thm
divides_refl_thm
divides_antisym_thm
divides_plus_thm
divides_times_thm
divides_≤_thm
divisors_finite_thm
divides_1_thm
mod_plus_homomorphism_thm
mod_times_homomorphism_thm
*mod_*ℕ*_exp_thm*
square_≤_mono_thm

We now specify the greatest common divisor function by requiring it to produce greatest lower bounds with respect to the divisor ordering.

HOL Constant

$$\begin{array}{|llll}
\multicolumn{4}{|l}{\boldsymbol{Gcd} : \mathbb{N} \to \mathbb{N} \to \mathbb{N}} \\
\hline
\forall m\ n \bullet & & 0 < m \lor 0 < n & \\
\Rightarrow & \multicolumn{3}{l}{Gcd\ m\ n\ Divides\ m \land Gcd\ m\ n\ Divides\ n} \\
\land & (\forall d \bullet & d\ Divides\ m \land d\ Divides\ n & \\
 & \Rightarrow & d\ Divides\ Gcd\ m\ n) &
\end{array}$$

We will need to prove the consistency of the above definition. Our approach is based on the one which exhibits the greatest common divisor of m and n as the smallest positive value of the form $am + bn$. To follow that approach directly requires a and b to range over both positive and 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 and is the method we use.

Various useful lemmas about greatest common divisors are then proved culminating in the theorem that Euclid's algorithm computes them.

Gcd_consistent
gcd_def
gcd_pos_thm
gcd_unique_thm
gcd_idemp_thm
gcd_comm_thm
gcd_plus_thm
gcd_eq_mod_thm
euclid_algorithm_thm

Now we define the set of prime numbers:

HOL Constant

$$\begin{array}{|l}
\boldsymbol{Prime} : \mathbb{N}\ SET \\
\hline
Prime = \{p \mid 1 < p \land \forall m\ n \bullet\ p = m{*}n \Rightarrow m = 1 \lor n = 1\}
\end{array}$$

The first important fact we need about prime numbers states 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 needed to develop the theory of the g.c.d.

prime_0_less_thm
prime_2_≤_thm
prime_divides_thm
gcd_prime_thm
prime_thm
prime_divisor_thm
prime_divisor_thm1

2.3 Indexed Sums and Products in $\mathbb{N}$

A useful application of the set fold operation is to define the following indexed sum operation. Given an index set, a, and a function, f, assigning a number to each member of a, $IndSum_N\ a\ f$ is the indexed sum $\sum_{x \in a} f(x)$, which is defined on any set a in which f has finite support.

HOL Constant

$$\mathbf{\mathit{IndSum_N}} : {}'a\ SET \to ({}'a \to \mathbb{N}) \to \mathbb{N}$$

$$\begin{array}{lll} \forall f\bullet & \mathit{IndSum}_N\ \{\}\ f = 0 & \\ \wedge & \forall x\ a\bullet & a \in \mathit{Finite} \wedge \neg x \in a \\ & \Rightarrow & \mathit{IndSum}_N\ (\{x\} \cup a)\ f = f\ x + \mathit{IndSum}_N\ a\ f \end{array}$$

We will write $\sum a\, f$ as shorthand for $\mathit{IndSum}_N\ a\ f$.

SML

```
declare_alias("Σ", ⌜IndSum_N⌝);
```

Similarly, we define indexed products:

HOL Constant

$$\mathbf{\mathit{IndProd_N}} : {}'a\ SET \to ({}'a \to \mathbb{N}) \to \mathbb{N}$$

$$\begin{array}{lll} \forall f\bullet & \mathit{IndProd}_N\ \{\}\ f = 1 & \\ \wedge & \forall x\ a\bullet & a \in \mathit{Finite} \wedge \neg x \in a \\ & \Rightarrow & \mathit{IndProd}_N\ (\{x\} \cup a)\ f = f\ x * \mathit{IndProd}_N\ a\ f \end{array}$$

We will write $\prod a\, f$ as shorthand for $\mathit{IndProd}_N\ a\ f$.

SML

```
declare_alias("Π", ⌜IndProd_N⌝);
```

The theorems about sums and products comprise various generalities that make the definitions useful in the common cases. Then as an exercise for the definitions, we prove the "division by 3 rule" which says that a number is divisible by 3 iff. the sum of its decimal digits is divisible by 3.

IndSum$_N$_consistent
ind_sum_ℕ_def
ind_sum_ℕ_0_thm
ind_sum_ℕ_local_thm
IndProd$_N$_consistent
ind_prod_ℕ_def
ind_prod_ℕ_1_thm
ind_prod_ℕ_0_thm
ind_prod_ℕ_local_thm
div_3_rule_thm1
div_3_rule_thm

Using indexed products, we can now give Euclid's proof that there are infinitely many primes:

prime_infinite_thm

2.4 Unique Factorisation in ℕ

The next group of theorems in the script prove the fundamental theorem of arithmetic, i.e., the statement that any positive natural number can be written uniquely as a product of prime powers.

The existence proof is standard, although it is very convenient to give an explicit formula for the exponent of a prime in the factorisation (*exponent_thm*). This makes the uniqueness part of the argument very simple.

prime_Π_thm
prime_divides_prime_thm
divides_ℕ_exp_thm
divides_cancel_thm
exponent_thm
unique_factorisation_thm
prime_divisors_unique_thm
prime_divisors_finite_thm

Having proved the above, we have the consistency of the following function that maps a non-zero number m and a prime p to the exponent of p in the prime factorisation of m.

HOL Constant

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

$$\begin{array}{ll} \forall m\bullet & 0 < m \\ \Rightarrow & \{p \mid \neg Exponent\ m\ p = 0\} \in Finite \\ \land & \{p \mid \neg Exponent\ m\ p = 0\} \subseteq Prime \\ \land & m = \Pi\ \{p \mid \neg\ Exponent\ m\ p = 0\}\ (\lambda\ p\bullet\ p\ \hat{}\ Exponent\ m\ p) \end{array}$$

2.5 Divergence of the Series of Prime Reciprocals

The next block of theorems lead up to the proof that the sum $\sum_p 1/p$ taken over all primes p diverges. This is done using essentially the argument given in Hardy and Wright [1]. It is convenient to define the notion of a square-free number, i.e., a number that is not divisible by a square other than 1.

HOL Constant

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

$$\forall m\bullet\ m \in SquareFree \Leftrightarrow \forall n\bullet\ n\hat{}2\ Divides\ m \Rightarrow n = 1$$

We first derive several facts about square-free numbers. In particular we show that a number is square-free iff. it is not divisible by the square of any prime. This shows that the non-zero exponents in the prime factorisation of a square-free number are all equal to 1. Using this, we show that given any finite set of primes P, the set of square-free number whose prime divisors lie in P is finite and has $2^{\#}\ (P)$ elements. We then show that every number can be written as a product $n^2 \times d$ where d is square-free.

square_free_0_less_thm
square_free_prime_thm
factorisation_square_free_thm
divides_square_free_thm
square_free_factorisation_thm
square_free_finite_size_thm
square_free_1_thm
square_free_divisor_thm
square_free_divisor_thm1

We now give a series of theorems that build up to the proof that $\sum_p 1/p$ taken over prime $p \leq n$ is unbounded as n tends to infinity. The argument is that of [1][Theorem 19] adapted to fit into the typed framework of HOL.

Consider a finite set of primes, P and a positive natural number n. If $m \leq n^2$, then either all prime divisors of m are in P or not. We will estimate the number of m falling under each of the two cases:

- If all the prime divisors of m lie in P, m can be written as $m = k^2 d$ where $k \leq n$ and where d is a square-free number whose prime divisors lie in P. There are at most n choices for k and $2^{\#(P)}$ so there are at most $n2^{\#(P)}$ such m.

- If m is divisible by a prime q that is not in P, we have $m = kq$ for some $k \leq n^2 \,\mathsf{div}\, q$. The number of such m is therefore $\sum_q n^2 \,\mathsf{div}\, q$ taken over all prime q with $q \notin P$ and $q \leq n^2$.

Let Q be the set of primes $q \leq n^2$ which are not in P, then, as any $m \leq n^2$ falls under one of the two cases, one has:

$$n^2 \quad \leq \quad n2^{\#(P)} + \sum_{q \in Q} n^2 \,\mathsf{div}\, q \tag{1}$$

Putting $n = 2^{\#(P)+1}$ this gives:

$$2^{2\#(P)+2} \quad \leq \quad 2^{2\#(P)+1} + \sum_{q \in Q} 2^{2\#(P)+2} \,\mathsf{div}\, q \tag{2}$$

Whence, subtracting $2^{2\#(P)+1}$ from both sides and then, observing that $i \,\mathsf{div}\, q \leq i/q$, and dividing through by $2^{2\#(P)+2}$, one has:

$$2^{2\#(P)+1} \quad \leq \quad \sum_{q \in Q} 2^{2\#(P)+2} \,\mathsf{div}\, q \tag{3}$$

$$1/2 \quad \leq \quad \sum_{q \in Q} 1/q \tag{4}$$

I.e., given any finite set of primes P, taking Q to be the set of primes q that are not in P and that satisfy $q \leq 2^{2\#(P)+2}$, the sum of reciprocals of the elements of Q is greater than $1/2$. That the sum of the series of reciprocals of the primes diverges follows by an easy induction (given any initial subsequence of the sequence of primes for which the sum or reciprocals is s, say, the above argument gives a longer initial subsequence whose sum is $s + 1/2$). The following block of theorems implement the above proof.

recip_primes_div_estimate_thm1
divisors_finite_size_thm
recip_primes_div_estimate_thm2
recip_primes_div_estimate_thm3
recip_primes_div_estimate_thm4
ℕℝ*_ind_sum_thm*
ind_sum_≤_mono_thm
ℕℝ*_div_≤_thm*
recip_primes_div_estimate_thm5
recip_primes_div_thm

2.6 Coprimality

SML

```
declare_infix(200, "Coprime");
```

HOL Constant

```
$Coprime : ℕ → ℕ → BOOL
────────────────────────────────
∀m n• m Coprime n ⇔ ∀i• i Divides m ∧ i Divides n ⇒ i = 1
```

coprime_prime_thm
coprime_gcd_thm

2.7 Real Integral Domains

In general, an integral domain is a ring without zero divisors. As we are only concerned with subrings of the reals here, any subring of the reals is an integral domain.

HOL Constant

$\boldsymbol{RealID} : \mathbb{R}\ \mathit{SET}\ \mathit{SET}$

$$
\begin{aligned}
&\forall A \bullet\ A \in \mathit{RealID} \Leftrightarrow\\
&\qquad \mathbb{NR}\ \mathit{1} \in A\\
&\wedge \qquad (\forall x\ y \bullet x \in A \wedge y \in A \Rightarrow x + y \in A)\\
&\wedge \qquad (\forall x \bullet x \in A \Rightarrow \sim x \in A)\\
&\wedge \qquad (\forall x\ y \bullet x \in A \wedge y \in A \Rightarrow x * y \in A)
\end{aligned}
$$

The domain of (rational) integers comprises the intersection of all real integral domains:

HOL Constant

$\mathbb{Z}_{\boldsymbol{R}} : \mathbb{R}\ \mathit{SET}$

$$\mathbb{Z}_R = \bigcap \mathit{RealID}$$

SML

```
declare_alias("ℤ", ⌜ℤ_R⌝);
```

To get started, we prove that ℝ is a real integral domain, as is the intersection of any family of real integral domains, and so in particular is ℤ, the intersection of all real integral domains. We then show that ℤ is precisely the image of the type ℤ of integers under the injection ℤℝ:

ℝ_real_i_d_thm
⋂_real_i_d_thm
ℤ_real_i_d_thm
ℤ_thm

2.8 Real Fields

A real field is a real integral domain that is closed under taking reciprocals of non-zero elements.

HOL Constant

$\boldsymbol{RealField} : \mathbb{R}\ \mathit{SET}\ \mathit{SET}$

$$
\begin{aligned}
&\forall A \bullet\ A \in \mathit{RealField} \Leftrightarrow\\
&\qquad A \in \mathit{RealID}\\
&\wedge \qquad (\forall x \bullet x \in A \setminus \{\mathbb{NR}\ \mathit{0}\} \Rightarrow x\ ^{-\mathit{1}} \in A)
\end{aligned}
$$

The field of rational numbes is the intersection of all real fields.

HOL Constant

$\mathbb{Q}_{\boldsymbol{R}} : \mathbb{R}\ \mathit{SET}$

$$\mathbb{Q}_R = \bigcap \mathit{RealField}$$

Following a similar pattern to the last section, we prove that $\mathbb{R}$ is a real field, as is the intersection of any family of real fields, in particular, $\mathbb{Q}$, the intersection of all real fields. We prove that $\mathbb{Z}$ is a subset of $\mathbb{Q}$. An explicit formula for the set $\mathbb{Q}$ is given in the next section.

ℝ_real_field_thm
⋂_real_field_thm
rat_real_i_d_thm
ℤ_⊆_rat_thm

SML

```
declare_alias("ℚ", ⌜ℚ_R⌝);
```

2.9 Fields of Fractions

The field of fractions of a set A, (typically an integral domain) is the intersection of all fields that contain A.

HOL Constant

FieldOfFractions : $\mathbb{R}\ SET \to \mathbb{R}\ SET$

$\forall A \bullet\ FieldOfFractions\ A = \bigcap\{K \mid K \in RealField \land A \subseteq K\}$

We prove that the field of fractions of any set is indeed a real field and that $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. We then show that if A is an integral domain, then its field of fractions does indeed comprise precisely the set of fractions a/b with $a, b \in A$ and $b \neq 0$. Using this we can derive an explicit formula for the set $\mathbb{Q}$.

field_of_fractions_field_thm
field_of_fractions_thm
rat_field_of_fractions_thm
rat_thm
rat_thm1

3 Irrationality of Quadratic Surds

We prove that any quadratic surd that is not an integer is irrational, and in particular, that $\sqrt{2}$ is irrational. The proof is as follows: 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 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. Thus to prove that $\sqrt{2}$ is irrational it suffices to show that it is not an integer.

sqrt_eq_thm
quadratic_surd_thm1
quadratic_surd_thm
sqrt_2_lemma
sqrt_2_irrational_thm

4 Arithmetic *modulo* a Prime

The next block of results develop some basic facts about arithemetic *modulo* prime numbers, e.g., the existence of multiplicative inverses *modulo* primes. The block concludes with Wilson's theorem: if $1 < p$, then p is prime iff. $(p-1)!$ is congruent to -1 *modulo* p. We state this in term of the mod operator on the natural numbers so that it becomes "p is prime iff. $(p-1)! \operatorname{mod} p = p - 1$".

plus_mod_thm
times_mod_p_inverse_thm
times_mod_p_inverse_thm1
times_mod_p_inverse_unique_thm
wilson_lemma1
wilson_thm

5 The Two Squares Theorem

The combinatorial part of the Heath-Brown proof of the two squares theorem is given in [2], with the various assumptions on the prime p made explicit. We complete the proof using the concept of primes defined in this document.

This involves transferring results from the type of integers to the type of natural numbers. The following function is convenient for doing the transfer.

HOL Constant

$\boldsymbol{Abs}_{\mathbb{N}} : \mathbb{Z} \to \mathbb{N}$

$\forall i \bullet \mathbb{N}\mathbb{Z}\ (Abs_{\mathbb{N}}\ i) = Abs\ i$

With some basic properties of the function $Abs_{\mathbb{N}}$ and one or two little lemmas about squares, we derive the two squares theorem from the combinatorial result of [2],

Abs$_{\mathbb{N}}$*_consistent*
abs_ℕ_thm
abs_ℕ_ℕℤ_thm
abs_ℕ_times_thm
abs_ℕ_cases_thm
ℤ_abs_square_thm
prime_¬_square_thm
two_squares_thm

References

[1] G.M. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, fifth edition, 1978.

[2] LEMMA1/HOL/WRK073. *Mathematical Case Studies: Some Finite Combinatorics.* R.D. Arthan, Lemma 1 Ltd., `rda@lemma-one.com`.

A THEOREMS IN THE THEORY numbers

max_∈_thm $\vdash \forall\ m\ n\ a \bullet\ (\forall\ i \bullet\ i \in a \Rightarrow i \leq m) \land n \in a \Rightarrow \mathit{Max}\ a \in a$

≤_max_thm $\vdash \forall\ m\ n\ a \bullet\ (\forall\ i \bullet\ i \in a \Rightarrow i \leq m) \land n \in a \Rightarrow n \leq \mathit{Max}\ a$

times_eq_0_thm

$\vdash \forall\ m\ n \bullet\ m * n = 0 \Leftrightarrow m = 0 \lor n = 0$

times_cancel_thm

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

times_eq_eq_1_thm

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

times_eq_1_thm

$\vdash \forall\ m\ n \bullet\ m * n = 1 \Leftrightarrow m = 1 \land n = 1$

ℕ***_exp_clauses***

$\vdash \forall\ m \bullet\ m\ \hat{}\ 0 = 1 \land m\ \hat{}\ 1 = m \land m\ \hat{}\ 2 = m * m$

ℕ***_exp_eq_0_thm***

$\vdash \forall\ m\ n \bullet\ m\ \hat{}\ n = 0 \Leftrightarrow m = 0 \land \neg\ n = 0$

ℕ***_exp_eq_1_thm***

$\vdash \forall\ m\ n \bullet\ m\ \hat{}\ n = 1 \Leftrightarrow m = 1 \lor n = 0$

ℕ***_exp_1_thm*** $\vdash \forall\ m \bullet\ m\ \hat{}\ 1 = m$

ℕ***_exp_divides_thm***

$\vdash \forall\ m\ k\ n \bullet\ k \leq n \Rightarrow m\ \hat{}\ k\ \mathit{Divides}\ m\ \hat{}\ n$

ℕ***_exp_times_thm***

$\vdash \forall\ m\ n\ k \bullet\ m\ \hat{}\ n * m\ \hat{}\ k = m\ \hat{}\ (n + k)$

ℕ***_exp_***ℕ***_exp_thm***

$\vdash \forall\ m\ n\ k \bullet\ (m\ \hat{}\ n)\ \hat{}\ k = m\ \hat{}\ (n * k)$

div_mod_1_thm

$\vdash \forall\ m \bullet\ m\ \mathit{Div}\ 1 = m \land m\ \mathit{Mod}\ 1 = 0$

m_div_mod_m_thm

$\vdash \forall\ m \bullet\ 0 < m \Rightarrow m\ \mathit{Div}\ m = 1 \land m\ \mathit{Mod}\ m = 0$

zero_div_mod_thm

$\vdash \forall\ m \bullet\ 0 < m \Rightarrow 0\ \mathit{Div}\ m = 0 \land 0\ \mathit{Mod}\ m = 0$

less_div_mod_thm

$\vdash \forall\ m\ n \bullet\ n < m \Rightarrow n\ \mathit{Div}\ m = 0 \land n\ \mathit{Mod}\ m = n$

div_mod_times_cancel_thm

$$\begin{array}{l}
\vdash \forall\ k\ m\ n \\
\quad \bullet\ 0 < k \\
\qquad \Rightarrow (m * k + n)\ \mathit{Div}\ k = m + n\ \mathit{Div}\ k \\
\qquad\quad \land (m * k + n)\ \mathit{Mod}\ k = n\ \mathit{Mod}\ k
\end{array}$$

mod_clauses

$$\begin{array}{l}
\vdash \forall\ k\ m\ n \\
\quad \bullet\ 0 < k \\
\qquad \Rightarrow (m * k)\ \mathit{Mod}\ k = 0 \\
\qquad\quad \land (k * m)\ \mathit{Mod}\ k = 0 \\
\qquad\quad \land (k * m + n)\ \mathit{Mod}\ k = n\ \mathit{Mod}\ k \\
\qquad\quad \land (m * k + n)\ \mathit{Mod}\ k = n\ \mathit{Mod}\ k \\
\qquad\quad \land (n + k * m)\ \mathit{Mod}\ k = n\ \mathit{Mod}\ k \\
\qquad\quad \land (n + m * k)\ \mathit{Mod}\ k = n\ \mathit{Mod}\ k \\
\qquad\quad \land (k + n)\ \mathit{Mod}\ k = n\ \mathit{Mod}\ k \\
\qquad\quad \land (n + k)\ \mathit{Mod}\ k = n\ \mathit{Mod}\ k \\
\qquad\quad \land 0\ \mathit{Mod}\ k = 0 \\
\qquad\quad \land k\ \mathit{Mod}\ k = 0 \\
\qquad\quad \land m\ \mathit{Mod}\ k\ \mathit{Mod}\ k = m\ \mathit{Mod}\ k
\end{array}$$

div_clauses

$$\begin{array}{l}
\vdash \forall\ k\\
\quad \bullet\ 0 < k\\
\qquad \Rightarrow (\forall\ m\\
\qquad\quad \bullet\ 0 < k\\
\qquad\qquad \Rightarrow (m * k)\ \mathit{Div}\ k = m\\
\qquad\qquad\quad \wedge\ (k * m)\ \mathit{Div}\ k = m\\
\qquad\qquad\quad \wedge\ 0\ \mathit{Div}\ k = 0\\
\qquad\qquad\quad \wedge\ k\ \mathit{Div}\ k = 1)\\
\qquad\quad \wedge\ (\forall\ m\ n\\
\qquad\quad \bullet\ n < k\\
\qquad\qquad \Rightarrow (k * m + n)\ \mathit{Div}\ k = m\\
\qquad\qquad\quad \wedge\ (m * k + n)\ \mathit{Div}\ k = m\\
\qquad\qquad\quad \wedge\ (n + k * m)\ \mathit{Div}\ k = m\\
\qquad\qquad\quad \wedge\ (n + m * k)\ \mathit{Div}\ k = m\\
\qquad\qquad\quad \wedge\ (k + n)\ \mathit{Div}\ k = 1\\
\qquad\qquad\quad \wedge\ (n + k)\ \mathit{Div}\ k = 1)
\end{array}$$

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

divides_mod_eq_0_thm

$\vdash \forall\ m\ n \bullet\ 0 < n \Rightarrow (n\ \mathit{Divides}\ m \Leftrightarrow m\ \mathit{Mod}\ n = 0)$

divides_0_thm

$\vdash \forall\ m \bullet\ m\ \mathit{Divides}\ 0 \wedge (0\ \mathit{Divides}\ m \Leftrightarrow m = 0)$

divides_mod_thm

$$\begin{array}{l}
\vdash \forall\ n\ m\\
\quad \bullet\ n\ \mathit{Divides}\ m \Leftrightarrow (\mathit{if}\ 0 < n\ \mathit{then}\ m\ \mathit{Mod}\ n\ \mathit{else}\ m) = 0
\end{array}$$

divides_refl_thm

$\vdash \forall\ m \bullet\ m\ \mathit{Divides}\ m$

divides_antisym_thm

$\vdash \forall\ m\ n \bullet\ n\ \mathit{Divides}\ m \wedge m\ \mathit{Divides}\ n \Leftrightarrow m = n$

divides_trans_thm

$\vdash \forall\ m\ n\ k \bullet\ n\ \mathit{Divides}\ m \wedge m\ \mathit{Divides}\ k \Rightarrow n\ \mathit{Divides}\ k$

divides_plus_thm

$$\begin{array}{l}
\vdash \forall\ m\ n\ d\\
\quad \bullet\ d\ \mathit{Divides}\ n \Rightarrow (d\ \mathit{Divides}\ m + n \Leftrightarrow d\ \mathit{Divides}\ m)
\end{array}$$

divides_times_thm

$\vdash \forall\ m\ d \bullet\ d\ \mathit{Divides}\ m * d \wedge d\ \mathit{Divides}\ d * m$

divides_≤_thm

$\vdash \forall\ m\ n \bullet\ 0 < m \wedge n\ \mathit{Divides}\ m \Rightarrow 0 < n \wedge n \leq m$

divisors_finite_thm

$\vdash \forall\ m \bullet\ 0 < m \Rightarrow \{d | d\ \mathit{Divides}\ m\} \in \mathit{Finite}$

divides_1_thm

$\vdash \forall\ m \bullet\ m\ \mathit{Divides}\ 1 \Leftrightarrow m = 1$

mod_plus_homomorphism_thm

$$\begin{array}{l}
\vdash \forall\ m\ n\ k\\
\quad \bullet\ 0 < k \Rightarrow (m + n)\ \mathit{Mod}\ k = (m\ \mathit{Mod}\ k + n\ \mathit{Mod}\ k)\ \mathit{Mod}\ k
\end{array}$$

mod_times_homomorphism_thm

$$\begin{array}{l}
\vdash \forall\ m\ n\ k\\
\quad \bullet\ 0 < k \Rightarrow (m * n)\ \mathit{Mod}\ k = (m\ \mathit{Mod}\ k * n\ \mathit{Mod}\ k)\ \mathit{Mod}\ k
\end{array}$$

mod_ℕ_exp_thm

$\vdash \forall\ m\ n\ k \bullet\ 0 < k \Rightarrow m\ \hat{}\ n\ \mathit{Mod}\ k = (m\ \mathit{Mod}\ k)\ \hat{}\ n\ \mathit{Mod}\ k$

square_≤_mono_thm

$\vdash \forall\ m\ n \bullet\ m \leq n \Leftrightarrow m\ \hat{}\ 2 \leq n\ \hat{}\ 2$

Gcd_consistent

$$\begin{array}{l}
\vdash \mathit{Consistent}\\
\quad (\lambda\ \mathit{Gcd}'\\
\quad\ \bullet \forall\ m\ n\\
\qquad \bullet\ 0 < m \lor 0 < n\\
\qquad\quad \Rightarrow \mathit{Gcd}'\ m\ n\ \mathit{Divides}\ m\\
\qquad\qquad \land\ \mathit{Gcd}'\ m\ n\ \mathit{Divides}\ n\\
\qquad\qquad \land\ (\forall\ d\\
\qquad\qquad \bullet\ d\ \mathit{Divides}\ m \land d\ \mathit{Divides}\ n\\
\qquad\qquad\quad \Rightarrow d\ \mathit{Divides}\ \mathit{Gcd}'\ m\ n))
\end{array}$$

gcd_def

$$\begin{array}{l}
\vdash \forall\ m\ n\\
\quad \bullet\ 0 < m \lor 0 < n\\
\qquad \Rightarrow \mathit{Gcd}\ m\ n\ \mathit{Divides}\ m\\
\qquad\quad \land\ \mathit{Gcd}\ m\ n\ \mathit{Divides}\ n\\
\qquad\quad \land\ (\forall\ d\\
\qquad\quad \bullet\ d\ \mathit{Divides}\ m \land d\ \mathit{Divides}\ n\\
\qquad\qquad \Rightarrow d\ \mathit{Divides}\ \mathit{Gcd}\ m\ n)
\end{array}$$

gcd_pos_thm

$$\vdash \forall\ m\ n \bullet\ 0 < m \lor 0 < n \Rightarrow 0 < \mathit{Gcd}\ m\ n$$

gcd_unique_thm

$$\begin{array}{l}
\vdash \forall\ m\ n\ d\\
\quad \bullet\ (0 < m \lor 0 < n)\\
\qquad\quad \land\ d\ \mathit{Divides}\ m\\
\qquad\quad \land\ d\ \mathit{Divides}\ n\\
\qquad\quad \land\ \mathit{Gcd}\ m\ n\ \mathit{Divides}\ d\\
\qquad \Rightarrow d = \mathit{Gcd}\ m\ n
\end{array}$$

gcd_idemp_thm

$$\vdash \forall\ m \bullet\ 0 < m \Rightarrow \mathit{Gcd}\ m\ m = m$$

gcd_comm_thm

$$\vdash \forall\ m\ n\ d \bullet\ 0 < m \lor 0 < n \Rightarrow \mathit{Gcd}\ m\ n = \mathit{Gcd}\ n\ m$$

gcd_plus_thm

$$\vdash \forall\ m\ n\ d \bullet\ 0 < m \lor 0 < n \Rightarrow \mathit{Gcd}\ (m + n)\ n = \mathit{Gcd}\ m\ n$$

gcd_eq_mod_thm

$$\begin{array}{l}
\vdash \forall\ m\ n\\
\quad \bullet\ 0 < m \land 0 < n \land 0 < m\ \mathit{Mod}\ n\\
\qquad \Rightarrow (\exists\ a\\
\qquad \bullet\ 0 < (a * m)\ \mathit{Mod}\ n\\
\qquad\qquad \land\ (\forall\ b\\
\qquad\qquad \bullet\ 0 < (b * m)\ \mathit{Mod}\ n\\
\qquad\qquad\quad \Rightarrow (a * m)\ \mathit{Mod}\ n \le (b * m)\ \mathit{Mod}\ n)\\
\qquad\qquad \land\ \mathit{Gcd}\ m\ n = (a * m)\ \mathit{Mod}\ n)
\end{array}$$

euclid_algorithm_thm

$$\begin{array}{l}
\vdash \forall\ m\ n\\
\quad \bullet\ 0 < m \land 0 < n\\
\qquad \Rightarrow \mathit{Gcd}\ m\ n\\
\qquad\quad = (\mathit{if}\ m < n\\
\qquad\qquad \mathit{then}\ \mathit{Gcd}\ m\ (n - m)\\
\qquad\qquad \mathit{else}\ \mathit{if}\ m = n\\
\qquad\qquad \mathit{then}\ m\\
\qquad\qquad \mathit{else}\ \mathit{Gcd}\ (m - n)\ n)
\end{array}$$

***bezout_thm*1**

$$\begin{array}{l}
\vdash \forall\ m\ n\\
\quad \bullet\ 0 < m \land 0 < n \land m \le n\\
\qquad \Rightarrow (\exists\ a\ b\\
\qquad \bullet\ b * n \le a * m \land \mathit{Gcd}\ m\ n = a * m - b * n)
\end{array}$$

bezout_thm

$$\begin{array}{l}
\vdash \forall\ m\ n \\
\quad \bullet\ 0 < m \land 0 < n \\
\qquad \Rightarrow (\exists\ a\ b \\
\qquad\quad \bullet\ b * n \le a * m \land Gcd\ m\ n = a * m - b * n) \\
\qquad\quad \lor (\exists\ a\ b \\
\qquad\quad \bullet\ a * m \le b * n \land Gcd\ m\ n = b * n - a * m)
\end{array}$$

prime_0_less_thm

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

prime_2_≤_thm

$$\vdash \forall\ p \bullet\ p \in Prime \Rightarrow 2 \le p$$

prime_divides_thm

$$\begin{array}{l}
\vdash \forall\ p \\
\quad \bullet\ p \in Prime \\
\qquad \Leftrightarrow 1 < p \land (\forall\ d \bullet\ d\ Divides\ p \Leftrightarrow d = 1 \lor d = p)
\end{array}$$

gcd_prime_thm

$$\vdash \forall\ m\ p \bullet\ 0 < m \land p \in Prime \Rightarrow Gcd\ m\ p = 1 \lor Gcd\ m\ p = p$$

prime_thm

$$\begin{array}{l}
\vdash \forall\ p \\
\quad \bullet\ p \in Prime \\
\qquad \Leftrightarrow 1 < p \\
\qquad\quad \land (\forall\ m\ n \\
\qquad\quad \bullet\ p\ Divides\ m * n \Rightarrow p\ Divides\ m \lor p\ Divides\ n)
\end{array}$$

***prime_divisor_thm*1**

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

prime_divisor_thm

$$\vdash \forall\ m \bullet\ 1 < m \Rightarrow (\exists\ p \bullet\ p \in Prime \land p\ Divides\ m)$$

IndSum$_N$_consistent

$$\begin{array}{l}
\vdash Consistent \\
\qquad (\lambda\ IndSum_N{}' \\
\qquad\quad \bullet\ \forall\ f \\
\qquad\qquad \bullet\ IndSum_N{}'\ \{\}\ f = 0 \\
\qquad\qquad\quad \land (\forall\ x\ a \\
\qquad\qquad\quad \bullet\ a \in Finite \land \neg\ x \in a \\
\qquad\qquad\qquad \Rightarrow IndSum_N{}'\ (\{x\} \cup a)\ f \\
\qquad\qquad\qquad\quad = f\ x + IndSum_N{}'\ a\ f))
\end{array}$$

ind_sum_ℕ_def

$$\begin{array}{l}
\vdash \forall\ f \\
\quad \bullet\ \Sigma\ \{\}\ f = 0 \\
\qquad \land (\forall\ x\ a \\
\qquad \bullet\ a \in Finite \land \neg\ x \in a \\
\qquad\quad \Rightarrow \Sigma\ (\{x\} \cup a)\ f = f\ x + \Sigma\ a\ f)
\end{array}$$

ind_sum_ℕ_0_thm

$$\begin{array}{l}
\vdash \forall\ A\ f \\
\quad \bullet\ A \in Finite \land \Sigma\ A\ f = 0 \Rightarrow (\forall\ x \bullet\ x \in A \Rightarrow f\ x = 0)
\end{array}$$

ind_sum_ℕ_local_thm

$$\begin{array}{l}
\vdash \forall\ A\ f\ g \\
\quad \bullet\ A \in Finite \land (\forall\ x \bullet\ x \in A \Rightarrow f\ x = g\ x) \\
\qquad \Rightarrow \Sigma\ A\ f = \Sigma\ A\ g
\end{array}$$

IndProd$_N$_consistent

$$\begin{array}{l}
\vdash Consistent \\
\qquad (\lambda\ IndProd_N{}' \\
\qquad\quad \bullet\ \forall\ f
\end{array}$$

$$\begin{array}{l}
\bullet\ \mathit{IndProd}_{N}'\ \{\}\ f = 1\\
\quad \land\ (\forall\ x\ a\\
\quad \bullet\ a \in \mathit{Finite} \land \neg\ x \in a\\
\qquad \Rightarrow \mathit{IndProd}_{N}'\ (\{x\} \cup a)\ f\\
\qquad\ = f\ x * \mathit{IndProd}_{N}'\ a\ f))
\end{array}$$

ind_prod_ℕ_def

$$\begin{array}{l}
\vdash \forall\ f\\
\ \bullet\ \mathit{\Pi}\ \{\}\ f = 1\\
\quad \land\ (\forall\ x\ a\\
\quad \bullet\ a \in \mathit{Finite} \land \neg\ x \in a\\
\qquad \Rightarrow \mathit{\Pi}\ (\{x\} \cup a)\ f = f\ x * \mathit{\Pi}\ a\ f)
\end{array}$$

ind_prod_ℕ_1_thm

$$\begin{array}{l}
\vdash \forall\ A\ f\\
\ \bullet\ A \in \mathit{Finite} \land \mathit{\Pi}\ A\ f = 1 \Rightarrow (\forall\ x \bullet\ x \in A \Rightarrow f\ x = 1)
\end{array}$$

ind_prod_ℕ_0_thm

$$\begin{array}{l}
\vdash \forall\ A\ f\\
\ \bullet\ A \in \mathit{Finite} \land \mathit{\Pi}\ A\ f = 0 \Rightarrow (\exists\ x \bullet\ x \in A \land f\ x = 0)
\end{array}$$

ind_prod_ℕ_local_thm

$$\begin{array}{l}
\vdash \forall\ A\ f\ g\\
\ \bullet\ A \in \mathit{Finite} \land (\forall\ x \bullet\ x \in A \Rightarrow f\ x = g\ x)\\
\quad \Rightarrow \mathit{\Pi}\ A\ f = \mathit{\Pi}\ A\ g
\end{array}$$

ind_prod_ℕ_clauses

$$\vdash \forall\ x\ f \bullet\ \mathit{\Pi}\ \{\}\ f = 1 \land \mathit{\Pi}\ \{x\}\ f = f\ x$$

ind_prod_ℕ_∪_thm

$$\begin{array}{l}
\vdash \forall\ a\ b\ f\\
\ \bullet\ a \in \mathit{Finite} \land b \in \mathit{Finite}\\
\quad \Rightarrow \mathit{\Pi}\ (a \cup b)\ f * \mathit{\Pi}\ (a \cap b)\ f = \mathit{\Pi}\ a\ f * \mathit{\Pi}\ b\ f
\end{array}$$

ind_prod_ℕ_disj_∪_thm

$$\begin{array}{l}
\vdash \forall\ a\ b\ f\\
\ \bullet\ a \in \mathit{Finite} \land b \in \mathit{Finite} \land a \cap b = \{\}\\
\quad \Rightarrow \mathit{\Pi}\ (a \cup b)\ f = \mathit{\Pi}\ a\ f * \mathit{\Pi}\ b\ f
\end{array}$$

ind_prod_ℕ_⋃_thm

$$\begin{array}{l}
\vdash \forall\ u\ f\\
\ \bullet\ u \in \mathit{Finite}\\
\qquad \land\ u \subseteq \mathit{Finite}\\
\qquad \land\ (\forall\ a\ b \bullet\ a \in u \land b \in u \land \neg\ a \cap b = \{\} \Rightarrow a = b)\\
\quad \Rightarrow \mathit{\Pi}\ (\bigcup\ u)\ f = \mathit{\Pi}\ u\ (\lambda\ a \bullet\ \mathit{\Pi}\ a\ f)
\end{array}$$

ind_prod_ℕ_mod_thm

$$\begin{array}{l}
\vdash \forall\ A\ f\ d\\
\ \bullet\ A \in \mathit{Finite} \land 0 < d\\
\quad \Rightarrow \mathit{\Pi}\ A\ f\ \mathit{Mod}\ d = \mathit{\Pi}\ A\ (\lambda\ k \bullet\ f\ k\ \mathit{Mod}\ d)\ \mathit{Mod}\ d
\end{array}$$

ind_prod_ℕ_k_1_thm

$$\vdash \forall\ A\ f \bullet\ A \in \mathit{Finite} \Rightarrow \mathit{\Pi}\ A\ (\lambda\ k \bullet\ 1) = 1$$

factorial_ind_prod_ℕ_thm

$$\vdash \forall\ m \bullet\ \mathit{\Pi}\ \{k | 1 \leq k \land k \leq m\}\ (\lambda\ k \bullet\ k) = m\ !$$

factorial_ind_prod_ℕ_thm1

$$\vdash \forall\ m \bullet\ 0 < m \Rightarrow (m - 1)\ ! = \mathit{\Pi}\ \{k | 1 \leq k \land k < m\}\ (\lambda\ k \bullet\ k)$$

div_3_rule_thm1

$$\begin{array}{l}
\vdash \forall\ \mathit{digits}\ n\\
\ \bullet\ \mathit{\Sigma}\ \{i | i < n\}\ (\lambda\ i \bullet\ \mathit{digits}\ i * 10\ \hat{}\ i)\ \mathit{Mod}\ 3\\
\quad = \mathit{\Sigma}\ \{i | i < n\}\ (\lambda\ i \bullet\ \mathit{digits}\ i)\ \mathit{Mod}\ 3
\end{array}$$

div_3_rule_thm

$$\begin{array}{l}
\vdash \forall\ \mathit{digits}\ n\\
\quad \bullet\ 3\ \mathit{Divides}\ \Sigma\ \{i|i < n\}\ (\lambda\ i\bullet\ \mathit{digits}\ i * 10 \mathbin{\hat{}} i)\\
\qquad \Leftrightarrow 3\ \mathit{Divides}\ \Sigma\ \{i|i < n\}\ (\lambda\ i\bullet\ \mathit{digits}\ i)
\end{array}$$

prime_2_thm $\vdash 2 \in \mathit{Prime}$

prime_infinite_thm

$$\vdash \neg\ \mathit{Prime} \in \mathit{Finite}$$

prime_Π_thm $\vdash \forall\ p\ A\ f$

$$\begin{array}{l}
\quad \bullet\ A \in \mathit{Finite} \land p \in \mathit{Prime} \land p\ \mathit{Divides}\ \Pi\ A\ f\\
\qquad \Rightarrow (\exists\ x\bullet\ x \in A \land p\ \mathit{Divides}\ f\ x)
\end{array}$$

prime_divides_prime_thm

$$\vdash \forall\ p\ q\bullet\ p \in \mathit{Prime} \land q \in \mathit{Prime} \land p\ \mathit{Divides}\ q \Rightarrow p = q$$

divides_ℕ_exp_thm

$$\begin{array}{l}
\vdash \forall\ p\ m\ n\\
\quad \bullet\ p \in \mathit{Prime} \land p\ \mathit{Divides}\ m \mathbin{\hat{}} n \Rightarrow m = 0 \lor p\ \mathit{Divides}\ m
\end{array}$$

divides_cancel_thm

$$\begin{array}{l}
\vdash \forall\ m\ n\ d\\
\quad \bullet\ \neg\ m = 0 \Rightarrow (d * m\ \mathit{Divides}\ m * n \Leftrightarrow d\ \mathit{Divides}\ n)
\end{array}$$

exponent_thm $\vdash \forall\ e$

$$\begin{array}{l}
\quad \bullet\ \{k|\neg\ e\ k = 0\} \in \mathit{Finite} \land \{k|\neg\ e\ k = 0\} \subseteq \mathit{Prime}\\
\qquad \Rightarrow (\forall\ k\\
\qquad \bullet\ e\ k\\
\qquad\quad = (\mathit{if}\ k \in \mathit{Prime}\\
\qquad\qquad \mathit{then}\\
\qquad\qquad\quad \mathit{Max}\\
\qquad\qquad\qquad \{i\\
\qquad\qquad\qquad\quad |k \mathbin{\hat{}} i\\
\qquad\qquad\qquad\qquad\quad \mathit{Divides}\ \Pi\\
\qquad\qquad\qquad\qquad\qquad \{k|\neg\ e\ k = 0\}\\
\qquad\qquad\qquad\qquad\qquad (\lambda\ p\bullet\ p \mathbin{\hat{}} e\ p)\}\\
\qquad\qquad \mathit{else}\ 0))
\end{array}$$

unique_factorisation_thm

$$\begin{array}{l}
\vdash \forall\ m\\
\quad \bullet\ 0 < m\\
\qquad \Rightarrow (\exists_1\ e\\
\qquad \bullet\ \{k|\neg\ e\ k = 0\} \in \mathit{Finite}\\
\qquad\quad \land \{k|\neg\ e\ k = 0\} \subseteq \mathit{Prime}\\
\qquad\quad \land m = \Pi\ \{k|\neg\ e\ k = 0\}\ (\lambda\ p\bullet\ p \mathbin{\hat{}} e\ p))
\end{array}$$

Exponent_consistent

$$\begin{array}{l}
\vdash \mathit{Consistent}\\
\quad (\lambda\ \mathit{Exponent}'\\
\quad \bullet\ \forall\ m\\
\qquad \bullet\ 0 < m\\
\qquad\quad \Rightarrow \{p|\neg\ \mathit{Exponent}'\ m\ p = 0\} \in \mathit{Finite}\\
\qquad\qquad \land \{p|\neg\ \mathit{Exponent}'\ m\ p = 0\} \subseteq \mathit{Prime}\\
\qquad\qquad \land m\\
\qquad\qquad\quad = \Pi\\
\qquad\qquad\qquad \{p|\neg\ \mathit{Exponent}'\ m\ p = 0\}\\
\qquad\qquad\qquad (\lambda\ p\bullet\ p \mathbin{\hat{}} \mathit{Exponent}'\ m\ p))
\end{array}$$

prime_divisors_unique_thm

$$\vdash \forall\ P\ Q\ e$$

$$\begin{array}{l}
\quad \bullet\ P \in \mathit{Finite} \\
\qquad\quad \land\ P \subseteq \mathit{Prime} \\
\qquad\quad \land\ Q \in \mathit{Finite} \\
\qquad\quad \land\ Q \subseteq \mathit{Prime} \\
\qquad\quad \land\ \mathit{\Pi}\ P\ (\lambda\ k\bullet\ k\ \hat{}\ (e\ k + \mathit{1})) \\
\qquad\qquad = \mathit{\Pi}\ Q\ (\lambda\ k\bullet\ k\ \hat{}\ (e\ k + \mathit{1})) \\
\qquad\quad \Rightarrow P = Q
\end{array}$$

prime_divisors_finite_thm

$$\vdash \forall\ m\bullet\ \mathit{0} < m \Rightarrow \{p | p \in \mathit{Prime} \land p\ \mathit{Divides}\ m\} \in \mathit{Finite}$$

square_free_0_less_thm

$$\vdash \forall\ m\bullet\ m \in \mathit{SquareFree} \Rightarrow \mathit{0} < m$$

square_free_prime_thm

$$\begin{array}{l}
\vdash \forall\ m \\
\quad \bullet\ m \in \mathit{SquareFree} \\
\qquad\quad \Leftrightarrow (\forall\ p\bullet\ p \in \mathit{Prime} \Rightarrow \neg\ p\ \hat{}\ \mathit{2}\ \mathit{Divides}\ m)
\end{array}$$

factorisation_square_free_thm

$$\begin{array}{l}
\vdash \forall\ P\ Q \\
\quad \bullet\ P \in \mathit{Finite} \land P \subseteq \mathit{Prime} \Rightarrow \mathit{\Pi}\ P\ (\lambda\ k\bullet\ k) \in \mathit{SquareFree}
\end{array}$$

divides_square_free_thm

$$\vdash \forall\ m\ d\bullet\ d\ \mathit{Divides}\ m \land m \in \mathit{SquareFree} \Rightarrow d \in \mathit{SquareFree}$$

square_free_factorisation_thm

$$\begin{array}{l}
\vdash \forall\ m \\
\quad \bullet\ m \in \mathit{SquareFree} \\
\qquad\quad \Rightarrow m = \mathit{\Pi}\ \{p | p \in \mathit{Prime} \land p\ \mathit{Divides}\ m\}\ (\lambda\ k\bullet\ k)
\end{array}$$

square_free_finite_size_thm

$$\begin{array}{l}
\vdash \forall\ P \\
\quad \bullet\ P \subseteq \mathit{Prime} \land P \in \mathit{Finite} \\
\qquad\quad \Rightarrow \{m \\
\qquad\qquad\quad | m \in \mathit{SquareFree} \\
\qquad\qquad\qquad\quad \land (\forall\ p\bullet\ p \in \mathit{Prime} \land p\ \mathit{Divides}\ m \Rightarrow p \in P)\} \\
\qquad\qquad\quad \in \mathit{Finite} \\
\qquad\qquad \land\ \# \\
\qquad\qquad\qquad \{m \\
\qquad\qquad\qquad\quad | m \in \mathit{SquareFree} \\
\qquad\qquad\qquad\qquad\quad \land (\forall\ p \\
\qquad\qquad\qquad\qquad\quad \bullet\ p \in \mathit{Prime} \land p\ \mathit{Divides}\ m \Rightarrow p \in P)\} \\
\qquad\qquad\quad = \mathit{2}\ \hat{}\ \#\ P
\end{array}$$

square_free_1_thm

$$\vdash \mathit{1} \in \mathit{SquareFree}$$

square_free_divisor_thm

$$\begin{array}{l}
\vdash \forall\ m \\
\quad \bullet\ \exists\ n\ d\bullet\ n\ \hat{}\ \mathit{2} \le m \land d \in \mathit{SquareFree} \land m = d * n\ \hat{}\ \mathit{2}
\end{array}$$

square_free_divisor_thm**1**

$$\begin{array}{l}
\vdash \forall\ m \\
\quad \bullet\ \mathit{0} < m \\
\qquad\quad \Rightarrow (\exists\ n\ d \\
\qquad\quad \bullet\ \mathit{0} < n \\
\qquad\qquad\quad \land\ \mathit{0} < d \\
\qquad\qquad\quad \land\ n\ \hat{}\ \mathit{2} \le m \\
\qquad\qquad\quad \land\ d \in \mathit{SquareFree} \\
\qquad\qquad\quad \land\ m = d * n\ \hat{}\ \mathit{2})
\end{array}$$

***recip_primes_div_estimate_thm*1**

$$\begin{array}{l}
\vdash \forall\ P\ n \\
\quad \bullet\ 0 < n \land P \subseteq \mathit{Prime} \land P \in \mathit{Finite} \\
\qquad \Rightarrow \{m \\
\qquad\quad |1 \leq m \\
\qquad\qquad \land\ m \leq n\ \hat{}\ 2 \\
\qquad\qquad \land\ (\forall\ p \bullet\ p \in \mathit{Prime} \land p\ \mathit{Divides}\ m \Rightarrow p \in P)\} \\
\qquad\quad \in \mathit{Finite} \\
\qquad\ \ \land\ \# \\
\qquad\qquad \{m \\
\qquad\qquad\ \ |1 \leq m \\
\qquad\qquad\qquad \land\ m \leq n\ \hat{}\ 2 \\
\qquad\qquad\qquad \land\ (\forall\ p \\
\qquad\qquad\qquad \bullet\ p \in \mathit{Prime} \land p\ \mathit{Divides}\ m \Rightarrow p \in P)\} \\
\qquad\quad \leq n * 2\ \hat{}\ \#\ P
\end{array}$$

divisors_finite_size_thm

$$\begin{array}{l}
\vdash \forall\ n\ d \\
\quad \bullet\ 0 < n \land 0 < d \\
\qquad \Rightarrow \{m|1 \leq m \land m \leq n \land d\ \mathit{Divides}\ m\} \in \mathit{Finite} \\
\qquad\ \ \land\ \#\ \{m|1 \leq m \land m \leq n \land d\ \mathit{Divides}\ m\} = n\ \mathit{Div}\ d
\end{array}$$

***recip_primes_div_estimate_thm*2**

$$\begin{array}{l}
\vdash \forall\ Q\ n \\
\quad \bullet\ Q \in \mathit{Finite} \land (\forall\ q \bullet\ q \in Q \Rightarrow 0 < q) \land 0 < n \\
\qquad \Rightarrow \{m \\
\qquad\quad |1 \leq m \\
\qquad\qquad \land\ m \leq n \\
\qquad\qquad \land\ (\exists\ q \bullet\ q \in Q \land q\ \mathit{Divides}\ m)\} \\
\qquad\quad \in \mathit{Finite} \\
\qquad\ \ \land\ \# \\
\qquad\qquad \{m \\
\qquad\qquad\ \ |1 \leq m \\
\qquad\qquad\qquad \land\ m \leq n \\
\qquad\qquad\qquad \land\ (\exists\ q \bullet\ q \in Q \land q\ \mathit{Divides}\ m)\} \\
\qquad\quad \leq \Sigma\ Q\ (\lambda\ q \bullet\ n\ \mathit{Div}\ q)
\end{array}$$

***recip_primes_div_estimate_thm*3**

$$\begin{array}{l}
\vdash \forall\ n\ P\ Q \\
\quad \bullet\ 0 < n \\
\qquad\ \ \land\ P \subseteq \mathit{Prime} \\
\qquad\ \ \land\ P \in \mathit{Finite} \\
\qquad\ \ \land\ Q = \{q|q \leq n\ \hat{}\ 2 \land q \in \mathit{Prime} \land \neg\ q \in P\} \\
\qquad \Rightarrow Q \in \mathit{Finite} \\
\qquad\ \ \land\ n\ \hat{}\ 2 \\
\qquad\quad \leq n * 2\ \hat{}\ \#\ P + \Sigma\ Q\ (\lambda\ q \bullet\ n\ \hat{}\ 2\ \mathit{Div}\ q)
\end{array}$$

***recip_primes_div_estimate_thm*4**

$$\begin{array}{l}
\vdash \forall\ P\ Q \\
\quad \bullet\ P \subseteq \mathit{Prime} \\
\qquad\ \ \land\ P \in \mathit{Finite} \\
\qquad\ \ \land\ Q \\
\qquad\quad = \{q \\
\qquad\quad |q \leq 2\ \hat{}\ (2 * \#\ P + 2) \land q \in \mathit{Prime} \land \neg\ q \in P\} \\
\qquad \Rightarrow Q \in \mathit{Finite}
\end{array}$$

$$\begin{array}{l}\qquad\quad \land\ 2\ \hat{}\ (2 * \#\ P + 1)\\ \qquad\qquad \leq \Sigma\ Q\ (\lambda\ q\bullet\ 2\ \hat{}\ (2 * \#\ P + 2)\ Div\ q)\end{array}$$

ℕℝ_ind_sum_thm

$$\vdash \forall\ A\ f\bullet\ A \in Finite \Rightarrow \mathbb{NR}\ (\Sigma\ A\ f) = \Sigma\ A\ (\lambda\ x\bullet\ \mathbb{NR}\ (f\ x))$$

ind_sum_≤_mono_thm

$$\begin{array}{l}\vdash \forall\ A\ f\ g\\ \quad \bullet\ A \in Finite \land (\forall\ x\bullet\ x \in A \Rightarrow f\ x \leq g\ x)\\ \qquad \Rightarrow \Sigma\ A\ f \leq \Sigma\ A\ g\end{array}$$

ℕℝ_div_≤_thm $\vdash \forall\ m\ n\bullet\ 0 < n \Rightarrow \mathbb{NR}\ (m\ Div\ n) \leq \mathbb{NR}\ m * \mathbb{NR}\ n\ ^{-1}$

***recip_primes_div_estimate_thm*5**

$$\begin{array}{l}\vdash \forall\ P\ Q\\ \quad \bullet\ P \subseteq Prime\\ \qquad\quad \land\ P \in Finite\\ \qquad\quad \land\ Q\\ \qquad\qquad = \{q\\ \qquad\qquad |q \leq 2\ \hat{}\ (2 * \#\ P + 2) \land q \in Prime \land \neg\ q \in P\}\\ \qquad \Rightarrow Q \in Finite \land 1\ /\ 2 \leq \Sigma\ Q\ (\lambda\ q\bullet\ \mathbb{NR}\ q\ ^{-1})\end{array}$$

recip_primes_div_thm

$$\begin{array}{l}\vdash (\forall\ n\bullet\ \{p|p \in Prime \land p \leq n\} \in Finite)\\ \quad \land\ (\forall\ m\\ \quad \bullet\ \exists\ n\\ \qquad \bullet\ \mathbb{NR}\ m\\ \qquad\qquad \leq \Sigma\ \{p|p \in Prime \land p \leq n\}\ (\lambda\ p\bullet\ \mathbb{NR}\ p\ ^{-1}))\end{array}$$

coprime_prime_thm

$$\begin{array}{l}\vdash \forall\ m\ n\\ \quad \bullet\ m\ Coprime\ n\\ \qquad \Leftrightarrow (\forall\ p\bullet\ p \in Prime \land p\ Divides\ m \Rightarrow \neg\ p\ Divides\ n)\end{array}$$

coprime_gcd_thm

$$\vdash \forall\ m\ n\bullet\ m\ Coprime\ n \Leftrightarrow (0 < m \lor 0 < n) \land Gcd\ m\ n = 1$$

ℝ_real_i_d_thm

$$\vdash Universe \in RealID$$

⋂_real_i_d_thm

$$\vdash \forall\ V\bullet\ V \subseteq RealID \Rightarrow \bigcap\ V \in RealID$$

ℤ_real_i_d_thm

$$\vdash \mathbb{Z} \in RealID$$

ℤ_thm $\vdash \mathbb{Z} = \{x|\exists\ i\bullet\ x = \mathbb{ZR}\ i\}$

ℝ_real_field_thm

$$\vdash Universe \in RealField$$

⋂_real_field_thm

$$\vdash \forall\ V\bullet\ V \subseteq RealField \Rightarrow \bigcap\ V \in RealField$$

rat_real_i_d_thm

$$\vdash \mathbb{Q} \in RealField$$

ℤ_⊆_rat_thm $\vdash \mathbb{Z} \subseteq \mathbb{Q}$

field_of_fractions_field_thm

$$\vdash \forall\ A\bullet\ FieldOfFractions\ A \in RealField$$

rat_field_of_fractions_thm

$$\vdash \mathbb{Q} = FieldOfFractions\ \mathbb{Z}$$

field_of_fractions_thm

$$\begin{array}{l}\vdash \forall\ A\\ \quad \bullet\ A \in RealID\\ \qquad \Rightarrow FieldOfFractions\ A\end{array}$$

$$\begin{array}{l}
\quad = \{x \\
\quad |\exists\ a\ b \\
\qquad \bullet\ a \in A \land b \in A \land \neg\ b = 0. \land x = a * b\ ^{-1}\}
\end{array}$$

rat_thm $\vdash \mathbb{Q} = \{x | \exists\ i\ m\bullet\ x = \mathbb{ZR}\ i * \mathbb{NR}\ (m + 1)\ ^{-1}\}$

***rat_thm*1** $\vdash \mathbb{Q} = \{x | \exists\ a\ b\bullet\ \neg\ b = 0 \land (x = a\ /\ b \lor x = \sim\ (a\ /\ b))\}$

sqrt_eq_thm $\vdash \forall\ x\ y\bullet\ 0. \le x \land x\ \hat{}\ 2 = y \Rightarrow x = Sqrt\ y$

***quadratic_surd_thm*1**

$$\begin{array}{l}
\vdash \forall\ k\ a\ b \\
\quad \bullet\ \neg\ b = 0 \land (a\ /\ b)\ \hat{}\ 2 = \mathbb{NR}\ k \\
\qquad \Rightarrow (\exists\ i\bullet\ \mathbb{NR}\ i\ \hat{}\ 2 = \mathbb{NR}\ k)
\end{array}$$

quadratic_surd_thm

$$\vdash \forall\ i\bullet\ 0. \le i \land i \in \mathbb{Z} \land Sqrt\ i \in \mathbb{Q} \Rightarrow Sqrt\ i \in \mathbb{Z}$$

sqrt_2_lemma $\vdash \neg\ Sqrt\ 2. \in \mathbb{Z}$

sqrt_2_irrational_thm

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

sqrt_1_mod_p_thm

$$\begin{array}{l}
\vdash \forall\ p\ m \\
\quad \bullet\ p \in Prime \land m < p \land m\ \hat{}\ 2\ Mod\ p = 1 \\
\qquad \Rightarrow m = 1 \lor p = m + 1
\end{array}$$

***sqrt_1_mod_p_thm*1**

$$\begin{array}{l}
\vdash \forall\ p \\
\quad \bullet\ p \in Prime \\
\qquad \Rightarrow 1 < p \\
\qquad\quad \land 1\ \hat{}\ 2\ Mod\ p = 1 \\
\qquad\quad \land 0 < p - 1 \\
\qquad\quad \land p - 1 < p \\
\qquad\quad \land (p - 1)\ \hat{}\ 2\ Mod\ p = 1
\end{array}$$

plus_mod_thm

$$\begin{array}{l}
\vdash \forall\ d\ m\ n \\
\quad \bullet\ 0 < d \land (m + n)\ Mod\ d = m\ Mod\ d \Rightarrow n\ Mod\ d = 0
\end{array}$$

times_mod_p_inverse_thm

$$\begin{array}{l}
\vdash \forall\ p\ m \\
\quad \bullet\ p \in Prime \land \neg\ p\ Divides\ m \\
\qquad \Rightarrow (\exists_1\ n\bullet\ n < p \land (m * n)\ Mod\ p = 1)
\end{array}$$

***times_mod_p_inverse_thm*1**

$$\begin{array}{l}
\vdash \forall\ p\ m \\
\quad \bullet\ p \in Prime \land 0 < m \land m < p \\
\qquad \Rightarrow (\exists_1\ n\bullet\ n < p \land (m * n)\ Mod\ p = 1)
\end{array}$$

times_mod_p_inverse_unique_thm

$$\begin{array}{l}
\vdash \forall\ p\ m\ n\ k \\
\quad \bullet\ p \in Prime \\
\qquad\quad \land 0 < m \\
\qquad\quad \land m < p \\
\qquad\quad \land 0 < n \\
\qquad\quad \land n < p \\
\qquad\quad \land 0 < k \\
\qquad\quad \land k < p \\
\qquad\quad \land ((m * n)\ Mod\ p = 1 \lor (n * m)\ Mod\ p = 1) \\
\qquad\quad \land ((m * k)\ Mod\ p = 1 \lor (k * m)\ Mod\ p = 1) \\
\qquad \Rightarrow n = k
\end{array}$$

***wilson_lemma*1**

$$\vdash \forall\ p$$

$\qquad\bullet\ p \in \mathit{Prime}$

$\qquad\quad \Rightarrow \mathit{\Pi}\ \{m | 1 < m \land m + 1 < p\}\ (\lambda\ m\bullet\ m)\ \mathit{Mod}\ p = 1$

wilson_thm $\vdash \forall\ p\bullet\ 1 < p \Rightarrow (p \in \mathit{Prime} \Leftrightarrow (p - 1)\ !\ \mathit{Mod}\ p = p - 1)$

Abs$_{\mathbb{N}}$_consistent

$\vdash \mathit{Consistent}$

$\qquad (\lambda\ \$"\mathit{Abs}_{\mathbb{N}}{}'"\bullet\ \forall\ i\bullet\ \mathbb{NZ}\ (\$"\mathit{Abs}_{\mathbb{N}}{}'"\ i) = \mathit{Abs}\ i)$

abs_$\mathbb{N}$_thm $\vdash \forall\ i\ m\bullet\ \mathit{Abs}_{\mathbb{N}}\ i = m \Leftrightarrow \mathit{Abs}\ i = \mathbb{NZ}\ m$

abs_$\mathbb{N}$_$\mathbb{NZ}$_thm $\vdash \forall\ m\bullet\ \mathit{Abs}_{\mathbb{N}}\ (\mathbb{NZ}\ m) = m \land \mathit{Abs}_{\mathbb{N}}\ (\sim (\mathbb{NZ}\ m)) = m$

abs_$\mathbb{N}$_times_thm

$\vdash \forall\ i\ j\bullet\ \mathit{Abs}_{\mathbb{N}}\ (i * j) = \mathit{Abs}_{\mathbb{N}}\ i * \mathit{Abs}_{\mathbb{N}}\ j$

abs_$\mathbb{N}$_cases_thm

$\vdash \forall\ i$

$\quad\bullet\ (\mathbb{NZ}\ 0 \le i \Rightarrow i = \mathbb{NZ}\ (\mathit{Abs}_{\mathbb{N}}\ i))$

$\qquad \land (\neg\ \mathbb{NZ}\ 0 \le i \Rightarrow i = \sim (\mathbb{NZ}\ (\mathit{Abs}_{\mathbb{N}}\ i)))$

$\mathbb{Z}$_abs_square_thm

$\vdash \forall\ i\bullet\ \mathit{Abs}\ i * \mathit{Abs}\ i = i * i$

prime_$\neg$_square_thm

$\vdash \forall\ p\ m\bullet\ p \in \mathit{Prime} \Rightarrow \neg\ p = m\ \hat{}\ 2$

two_squares_thm

$\vdash \forall\ p\ m$

$\quad\bullet\ p \in \mathit{Prime} \land p = 4 * m + 1$

$\qquad \Rightarrow (\exists\ a\ b\bullet\ p = a\ \hat{}\ 2 + b\ \hat{}\ 2)$

INDEX