Integeral Arithmetics

Uncultured Trump

December 28, 2018

Contents

1 Natural Numbers

1.1 Peano Axioms

$\texttt{NaturalSet} :: ?\sum N \in \mathsf{SET} \,.\, N \times (N \hookrightarrow N)$

$(N, 1, \sigma) : \texttt{NaturalSet} \iff \forall n \in N \,.\, \sigma(n) \neq 1 \,\&$

$\quad \& \,\forall P \subset N \,.\, \Big(1 \in P \,\&\, \forall n \in P \,.\, \sigma(n) \in P\Big) \Rightarrow P = N$

$\texttt{NaturalSetAsSet} :: \texttt{NaturalSet} \to \mathsf{SET}$

$\texttt{NaturalSetAsSet}\,(N, 1, \sigma) = (N, 1, \sigma) := N$

$\texttt{first} :: \prod N : \texttt{NaturalSet} \,.\, N$

$\texttt{first}\,(N, 1, \sigma) = 1_{N,1,\sigma} := 1$

$\texttt{next} :: \prod N : \texttt{NaturalSet} \,.\, N \hookrightarrow N$

$\texttt{next}\,((N, 1, \sigma), n) = n + 1 := \sigma(n)$

$\texttt{Succesors} :: \prod N : \texttt{NaturalSet} \,.\, ?N$

$m : \texttt{Succesors} \iff \exists n \in N \,.\, m = \sigma(n)$

$\texttt{StuctureOfNat} :: \forall N : \texttt{NaturalSet} \,.\, N = \{1_N\} \sqcup \texttt{Succesors}(N)$

$\texttt{Proof} \;=$

$(1) := \eth\texttt{NaturalSet}(N) : \{1_N\} \cap \texttt{Succesors}(N) = \emptyset,$

$P := \{1_N\} \sqcup \texttt{Succesors}(N) :?N,$

$\texttt{Assume}\; n : P,$

$(2) := \eth\texttt{Succesors}(N) : \sigma(n) \in \texttt{Succesors}(N),$

$() := \eth P(2) : \sigma(n) \in P;$

$\rightsquigarrow (2) := I(\forall) : \forall n \in P \,.\, \sigma(n) \in P,$

$(3) := \eth P(1_N) : 1_N \in P,$

$(*) := \eth N(2, 3) : N = P;$

$\square$

$\texttt{PrimitiveRecursiveDefinition} :: \forall N : \texttt{NaturalSet} \,.\, \forall X \in \mathsf{SET} \,.\, \forall x \in X \,.\, \forall g : X \times X \to N \,.$

$\quad .\, \exists! f : N \to X : f(1) = x \,\&\, \forall n \in N \,.\, f(\sigma(n)) = g(f(n))$

$\texttt{Proof} \;=$

$\dots$

$\square$

$\texttt{rec} :: \prod N : \texttt{NaturalSet} \,.\, \prod X \in \mathsf{SET} \,.\, X \times (X \to N) \to (N \to X)$

$\texttt{rec}\,(x, g) := \texttt{PrimitiveRecursiveDefinition}$

$\texttt{primPart} :: \prod N : \texttt{NaturalSet} \,.\, N \to ?N$

$\texttt{primPart}\,() = n := \texttt{rec}\Big(\{1\}.\Lambda M \in ?N \,.\, \sigma(M) \sqcup \{1\}\Big)$

$\texttt{StructureOfNat2} :: \forall N : \texttt{NaturalSet} \,.\, N = \bigcup_{n \in N} n$

$\texttt{Proof} \;=$

$P := \bigcup_{n \in N} n :?N,$

$(1) := \eth\texttt{singleton}(1_N) : 1_N \in \{1_N\},$

$(2) := \eth\texttt{promPart}(1_N)(1_N) : 1_N \in 1_N,$

$(3) := \eth P(2) : 1_N \in P,$

$\texttt{Assume}\; n : P,$

$(m, 4) := \eth P(n) : \sum m \in N \,.\, n \in m,$

$(5) := \texttt{Map}(4)(\sigma) : \sigma(n) \in \sigma(\texttt{primPart}(m)),$

$(6) := \eth\texttt{primPart}(5) : \sigma(n) \in \texttt{primPart}(\sigma(m)),$

$() := \eth P(6) : \sigma(n) \in P;$

$\rightsquigarrow (4) := I(\forall) : \forall n \in P \,.\, \sigma(n) \in P,$

$(*) := \eth N(3, 4) : N = P;$

$\square$

$\texttt{SelfContainment} :: \forall N : \texttt{NaturalSet} \,.\, \forall n \in N \,.\, n \in n$

$\texttt{Proof} \;=$

$P := \{n \in N : n \in n\} :?N,$

$(1) := \eth\texttt{primPart}(1_N) : 1_N \in P,$

$\texttt{Assume}\; n : P,$

$(2) := \eth P(n) : n \in \texttt{primPart}(n),$

$(3) := \eth\texttt{primPart}(\sigma(n)) : \texttt{primPart}(\sigma(n)) = \sigma(\texttt{primPart}),$

$(4) := \sigma(2) : \sigma(n) \in \sigma(\texttt{primPart}(n)),$

$(5) := (3)(4) : \sigma(n) \in \texttt{primPart}(\sigma(n)),$

$() := \eth P(5) : \sigma(n) \in P;$

$\rightsquigarrow (2) := I(\forall) : \forall n \in P \,.\, \sigma(n) \in P,$

$(*) := \eth\texttt{NaturalSet}(1, 2) : P = N;$

$\square$

$\texttt{PrimitiveSetNonEmpty} :: \forall N : \texttt{NaturalSet} \,.\, \forall n \in N \,.\, n \neq \emptyset$

$\texttt{Proof} \;=$

$\ldots$

$\square$

$\texttt{PrimitiveSetInjective} :: \forall N : \texttt{NatatturalSet} \;.\; \texttt{primPart}(N) : N \hookrightarrow ?N$

$\texttt{Proof} \;=$

$P := \{n \in \mathbb{N} : \forall m \in \mathbb{N} \;.\; \texttt{primPart}(m) = \texttt{primPart}(n) \Rightarrow m = n\} :?N,$

$\texttt{Assume}\; m : N,$

$\texttt{Assume}\; (1) : m = \{1\},$

$(2) := \texttt{SelfContaiment}(1) : m \in \{1\},$

$(3) := \eth\texttt{Singleton}(2) : m = 1;$

$\rightsquigarrow (4) := I(\forall)I(\Rightarrow)\eth P : 1 \in P,$

$\texttt{Assume}\; n : P,$

$\texttt{Assume}\; m : N,$

$\texttt{Assume}\; (2) : \texttt{primPart}(\sigma(n)) = \texttt{primPart}(m),$

$(3) := \eth\texttt{primPart}(\sigma(n)) : \sigma\big(\texttt{primPart}(n)\big) \subset \texttt{primPart}(\sigma(n)),$

$(4) := (2)(3)\texttt{Selfcontainment} : \sigma(n) \in \texttt{primPart}(m),$

$(k, 5) := \texttt{StructureOfNat}\eth\texttt{primPart}(4) : \sum k \in N \;.\; \sigma(k) = m,$

$(6) := \eth\texttt{NaturalSet}(5)(2) : \texttt{primPart}(k) = \texttt{primPart}(m),$

$(7) := \eth P(6) : k = n,$

$(8) := \sigma(7)(5) : \sigma(n) = m;$

$\rightsquigarrow (2) := \eth P I(\forall)) : \forall n \in P \;.\; \sigma(n) \in P,$

$(*) := \eth\texttt{NaturalSet}(N)(1, 2) : N = P;$

$\square$

$\texttt{PrimitiveSetIsFinite} :: \forall N : \texttt{NaturalSet} \;.\; \forall n \in \mathbb{N} \;.\; |\texttt{primPart}(n)| < \infty$

$\texttt{Proof} \;=$

$P := \{n \in N : |n| < \infty\} :?N,$

$(1) := \texttt{SingletonFinite}(1_N)\eth P : 1 \in P,$

$\texttt{Assume}\; n : P,$

$(2) := \eth P(n) : |n| < \infty,$

$(3) := \texttt{CardImage}(n, \sigma)(2) : |\sigma\; FUNCprimPart(n)| < \infty,$

$(4) := \texttt{SingleTonFinite}(1_N) : |\{1_N\}| < \infty,$

$(5) := \eth\texttt{primPartFiniteUnion}(3)(4) : |\texttt{primPart}(\sigma(n))| = |\sigma\; \texttt{PrimPart}(n) \cap \{1_N\}| < \infty,$

$() := \eth P(5) : \sigma(n) \in n;$

$\rightsquigarrow (2) := I(\forall) : \forall n \in P \;.\; \sigma(n) \in P,$

$(*) := \eth\texttt{NaturalSet}(N)(1, 2) : N = P;$

$\square$

$\texttt{AllNatsAreIso} :: \forall N, M : \texttt{NaturalSet} \,.\, N \cong_{\mathsf{SET}} M$

$\texttt{Proof} \ =$

$f := \texttt{rec}(N, M)(1_M, \Lambda m \in M \,.\, \sigma_M(m)) : N \to M,$

$(1) := \eth f(1_M) : 1_M \in \operatorname{Im} f,$

$\texttt{Assume}\ m : \operatorname{Im} f,$

$(n, 2) := \eth \operatorname{Im} f : \sum n \in N \,.\, f(n) = m,$

$(3) := \eth f(2) : f(\sigma(n)) = \sigma(f(n)) = \sigma(m),$

$() := \eth^{-1} \operatorname{Im}(3) : \sigma(m) \in \operatorname{Im} f;$

$\rightsquigarrow (2) := I(\forall) : \forall m \in \operatorname{Im} f \,.\, \sigma(m) \in \operatorname{Im} f,$

$(3) := \eth\texttt{NaturalSet}(M)(1, 2) : \operatorname{Im} f = M,$

$(4) := \eth^{-1}\texttt{Surjection}(f)(3) : \Big[f : N \twoheadrightarrow M\Big],$

$P := \{m \in M : |f^{-1}(m)| = 1\} :?M,$

$(5) := \texttt{StructureOfNat}(M)\eth f : 1_M \in P,$

$\texttt{Assume}\ m : P,$

$(n, 6) := (3)(m) : \sum n \in N \,.\, f(n) = m,$

$\texttt{Assume}\ k : N,$

$\texttt{Assume}\ (7) : f(k) = \sigma(m),$

$\texttt{Assume}\ (8) : k = 1_N,$

$(9) := \eth f(8)(7) : \sigma(m) = f(k) = f(1_N) = 1_M,$

$(10) := \eth^{-1}\texttt{Succesor}(M)(10) : 1_M \in \texttt{Succesor}(M),$

$() := \texttt{StructureOfNat}(M)(11) : \perp;$

$\rightsquigarrow (8) := E(\perp) : k \neq 1_N,$

$(9) := \texttt{StructureOfNat}(N)(8) : k \in \texttt{Succesor}(N),$

$(l, 10) := \eth\texttt{Succesor}(N)(9) : \sum l \in N \,.\, k = \sigma(l),$

$(11) := \eth f(10) : \sigma(m) = f(k) = \sigma(f(l)),$

$(12) := \eth\texttt{Injection}(\sigma)(11) : f(l) = m,$

$(13) := \eth P(12, 6)) : l = n,$

$() := \sigma(13)(10) : k = \sigma(n);$

$\rightsquigarrow (7) := I(\forall)\eth^{-1}|f^{-1}\{\sigma(m)\}| : |f^{-1}\{\sigma(m)\}| = |\{\sigma(n)| = 1,$

$() := \eth P(7) : \sigma(m) \in P;$

$\rightsquigarrow (6) := I(\forall) : \forall m \in P \,.\, \sigma(m) \in P,$

$(7) := \eth\texttt{NaturalSet}(M)(1, 2) : P = M,$

$(8) := \eth^{-1}\texttt{Bijection}(4)\eth^{-1}\texttt{Injection}(5)(7)\eth P : \Big[f : N \leftrightarrow M\Big],$

$(*) := \eth^{-1}\texttt{Isomorphic}(\mathsf{SET})(8) : N \cong_{\mathsf{SET}} M;$

$\square$

$\texttt{Assume}\ \mathbb{N} : \texttt{NaturalSet},$

1.2 Finite Induction

$\texttt{LinearlyInductive} :: ?\sum A : \mathsf{SET} \,.\, \sum P, S :?A \,.\, P \times (P \to S)$

$(A, P, S, 1, \sigma) : \texttt{Linearl tInductive} \iff \forall B \subset A \,.\, \Big(1 \in B \;\&\; \forall b \in B \cap P \,.\, \sigma(b) \in B\Big) \Rightarrow B = A$

$\texttt{HasFirst} :: \forall n \in \mathbb{N} \,.\, 1 \in n$

$\texttt{Proof} \;=$

$\dots$

$\square$

$\texttt{FiniteInductionIsWellDefined} :: \forall n \in \mathbb{N} \,.\, \forall m \in n \,.\, m \neq n \Rightarrow m + 1 \in n$

$\texttt{Proof} \;=$

$P := \{n \in \mathbb{N} : \forall m \in n \,.\, m \neq n \Rightarrow m + 1 \in n\} :?\mathbb{N},$

$\texttt{Assume}\ m : 1,$

$\texttt{Assume}\ (1) : m \neq 1_{\mathbb{N}},$

$(2) := \texttt{NotInSingleton}(1_{\mathbb{N}})(1) : m \notin 1_{\mathbb{N}},$

$(3) := I(\bot)(1)(2) : \bot,$

$(4) := E(\bot)(\sigma(m) \in 1_{\mathbb{N}}) : m + 1 \in 1_{\mathbb{N}};$

$\rightsquigarrow (1) := I(\forall)\eth^{-1}(P) : 1 \in P,$

$\texttt{Assume}\ n : P,$

$\texttt{Assume}\ m : n + 1,$

$\texttt{Assume}\ (2) : m \neq n + 1,$

$\texttt{Assume}\ (3) : m = 1_{\mathbb{N}},$

$(4) := \texttt{HasFirst}(n) : 1_{\mathbb{N}} \in n,$

$() := (3)\eth\texttt{primSet}(n + 1)(4) : m + 1 \in n + 1;$

$\rightsquigarrow (2) := I(\Rightarrow) : m = 1_{\mathbb{N}} \Rightarrow m + 1 \in n + 1,$

$\texttt{Assume}\ (3) : m \in \mathbb{N} + 1,$

$(k, 4)) := \eth\texttt{Succesors}(\mathbb{N})(m) : \sum k \in \mathbb{N} \,.\, k + 1 = m,$

$(5) := \eth\texttt{primSet}(n + 1)(m)(3)(4) : k \in n,$

$(6) := \eth\texttt{Injective}(\sigma)(2)(4) : k \neq n,$

$(7) := \eth P(6)(4) : m = k + 1 \in n,$

$(*) := \eth\texttt{primSet}(n + 1)(7) : m + 1 \in n + 1;$

$\rightsquigarrow (3) := I(\forall) : m \in \mathbb{N} + 1 \Rightarrow m + 1 \in n + 1,$

$() := \texttt{StructureOfNat}(\mathbb{N})E(|)(2)(3) : m + 1 \in n + 1;$

$\rightsquigarrow (2) := \eth^{-1}PI(\forall) : \forall n \in P \,.\, n + 1 \in P,$

$(3) := \eth^{-1}\texttt{NaturalSet}(\mathbb{N})(1)(2) : \mathbb{N} = P;$

$\square$

$\texttt{OverflowLemma} :: \forall n \in \mathbb{N} \,.\, n+1 \notin n$

$\texttt{Proof} \ =$

$P := n \in \mathbb{N} : n+1 \notin n :?\mathbb{N},$

$(2) := \eth\texttt{NaturalSet}(\mathbb{N}) : 1+1 \neq 1,$

$(3) := \texttt{NotInSingleton}(1)(2) : 1+1 \notin 1,$

$\texttt{Assume}\ n : P,$

$(4) := \eth P(n) : n+1 \notin P,$

$\texttt{Assume}\ (5) : n+1+1 \in n+1,$

$(6) := \eth\texttt{NaturalSet}(n+1+1) : n+1+1 \neq 1,$

$(7) := \eth\texttt{primPart}(n+1)(5,6) : n+1 \in n,$

$() := (7)(4) : \bot;$

$\rightsquigarrow (5) := E(\bot) : n+1+1 \notin n+1,$

$(6) := \eth P(5) : n+1 \in P;$

$\rightsquigarrow (4) := I(\forall) : \forall n \in P \,.\, n+1 \in P,$

$(*) := \eth\texttt{NaturalNumbers}(\mathbb{N})(3,4) : P = N;$

$\square$

$\texttt{PrimHasPreds} :: \forall n \in \mathbb{N} \,.\, \forall m+1 \in n \,.\, m \in n$

$\texttt{Proof} \ =$

$P := \{n \in \mathbb{N} : \forall m+1 \in n \,.\, m \in n\} :?\mathbb{N},$

$\texttt{Assume}\ m+1 : 1,$

$(1) := \eth\texttt{NaturalSet}(\mathbb{N})(m+1) : m+1 \neq 1,$

$(2) := \texttt{NotInSingleti}\Big(\texttt{primSet}(1)\Big)(1) : m+1 \notin 1,$

$(3) := (2)(m+1) : \bot,$

$() := E(\bot) : m \in 1;$

$\rightsquigarrow (1) := I(\forall)\eth P : 1 \in P,$

$\texttt{Assume}\ n : P,$

$\texttt{Assume}\ m+1 : n+1,$

$\texttt{Assume}\ (2) : m = 1,$

$() := \texttt{HasFirst}(n+1)(2) : m \in n+1;$

$\rightsquigarrow (2) := I(\Rightarrow) : m = 1 \Rightarrow m \in n+1,$

$\texttt{Assume}\ (3) : m \in \mathbb{N}+1,$

$(k,4) := \eth\texttt{Succesor}(\mathbb{N})(m) : \sum k \in \mathbb{N} \,.\, m = k+1,$

$(5) := \eth\texttt{primPart}(n+1)(m+1) : m \in n,$

$(6) := \eth P(n)(5)(4) : k \in n,$

$() := \eth\texttt{primPart}(n+1)(6)(4) : m \in n;$

$\rightsquigarrow (2) := \texttt{StructureOfNat}(\mathbb{N})E(|)(2) : \forall n \in P \,.\, n+1 \in P,$

$(*) := \eth\texttt{NaturalSet}(1)(2) : \mathbb{N} = P;$

$\square$

$\texttt{FiniteInduction} :: \forall n \in \mathbb{N} \,.\, (n, n \setminus \{n\}, n \setminus \{1\}, 1, \sigma) : \texttt{LinearlyInductive}$

$\texttt{Proof} \ =$

$\texttt{Assume}\ B :?n,$

$\texttt{Assume}\ (2) : 1 \in B,$

$\texttt{Assume}\ (3) : \forall m \in n \,.\, m \neq n \Rightarrow m + 1 \in B,$

$B' := B \cup n^{\complement} :?\mathbb{N},$

$(4) := (2)\eth\texttt{union} : 1 \in B',$

$\texttt{Assume}\ m : B',$

$\texttt{Assume}\ (5) : m \in n,$

$\texttt{Assume}\ (6) : m \neq n,$

$(7) := (3)(5)(6)(m) : m + 1 \in B,$

$() := \eth B'\eth\texttt{union}(7) : m + 1 \in B';$

$\rightsquigarrow (6) := I(\Rightarrow) : m \neq n \Rightarrow m \in B',$

$\texttt{Assume}\ (7) : m = n,$

$(8) := \texttt{overflowLemma}(n) : n + 1 \notin n,$

$(9) := \eth\texttt{complement}(\mathbb{N})(n)(8) : n + 1 \in n^{\complement},$

$() := \eth B'\eth\texttt{union}(9)(7) : m + 1 \in B';$

$\rightsquigarrow (7) := I(\Rightarrow) : m = n \Rightarrow m + 1 \in B',$

$() := \texttt{AllButOne}(n, n)E(|)(6, 7) : m + 1 \in B';$

$\rightsquigarrow (5) := I(\Rightarrow) : m \in n \Rightarrow m + 1 \in B',$

$\texttt{Assume}\ (6) : m \in n^{\complement},$

$\texttt{Assume}\ (7) : m + 1 \in n,$

$(8) := \texttt{PrimHasPreds}(7) : m \in n,$

$() := (6)(8) : \perp;$

$\rightsquigarrow (7) := E(\perp) : m + 1 \in n^{\complement},$

$() := \eth B'\eth\texttt{union} : m + 1 \in B';$

$\rightsquigarrow (6) := I(\Rightarrow) : m \in n^{\complement} \Rightarrow m + 1 \in B',$

$() := \texttt{FullAlternative}(\mathbb{N})(n)E(|)(5, 6) : m + 1 \in B';$

$(5) := I(\forall) : \forall m \in \mathbb{N} \,.\, m + 1 \in B',$

$(6) := \eth\texttt{NaturalSet}(4, 5) : B' = \mathbb{N},$

$() := (6)\texttt{UniversumIntersect}(n)(6)\texttt{UnionCancelation}(B, n^{\cap})\texttt{SubsetUntersect}(B, n) :$

$\quad : n = B' \cap n = (B \cup n^{\cap}) \cap n = B \cap n = n;$

$\rightsquigarrow (*) := I(\forall)I(\Rightarrow)\eth^{-1}\texttt{LinearlyInductive} : \Big[(n, n \setminus \{n\}, n \setminus \{1\}, 1, \sigma) : \texttt{LinearlyInductive}\Big];$

$\square$

1.3 Order Structure

$\texttt{NaturalOrder} :: ?(\mathbb{N} \times \mathbb{N})$

$(n, m) : \texttt{NaturalOrder} \iff n \subset m$

$\texttt{NaturalOrderIsOrder} :: \texttt{NaturalOrder} : \texttt{Order}$

$\texttt{Proof} \ =$

Use the fact that subsets of N are poset and the injectivity of the primitive sets

$\square$

$\texttt{orderedNaturalNumbers} :: \texttt{Poset}$

$\texttt{orderedNaturalNumbers}\,(\mathbb{N}) = (\mathbb{N}, \leq) := (\mathbb{N}, \texttt{NaturalOrder})$

$\texttt{FirstIsLowerBound} :: 1 : \texttt{LowerBound}(\mathbb{N})$

$\texttt{Proof} \ =$

$\texttt{Assume}\ m : \mathbb{N},$

$(1) := \eth\texttt{StructureOfNat}(\mathbb{N})(m) : m = 1 | m \in \texttt{Succesors}(\mathbb{N}),$

$\texttt{Assume}\ (2) : m = 1,$

$() := \eth\texttt{Reflexive}(\texttt{NaturalOrder})(m, 1)(1) : 1 \leq m;$

$\leadsto (2) := I(\Rightarrow) : m = 1 \Rightarrow 1 \leq m,$

$\texttt{Assume}\ (3) : \Big[m : \texttt{Succesor}(\mathbb{N})\Big],$

$(k, 4) := \eth\texttt{Succesor}(\mathbb{N})(m) : \sum k \in \mathbb{N}\ .\ m = \sigma(k),$

$(5) := \eth\texttt{primSet}(m)(4) : \texttt{primSet}(m) = \sigma(\texttt{primSet} k) \cup \{1\},$

$(6) := \eth\texttt{union}(5)\eth^{-1} 1 : 1 \in m,$

$(7) := \texttt{SingletonSubset}(6) : \{1\} \subset m,$

$() := \eth^{-1}\texttt{NaturalOrder}(7) : 1 \leq m;$

$\leadsto (3) := I(\rightarrow) : m \in \mathbb{N} + 1 \Rightarrow 1 \leq m,$

$() := E(|)(1, 2, 3) : 1 \leq m;$

$\leadsto (*) := \eth^{-1}\texttt{LowerBound} : \Big[1 : \texttt{LowerBound}(\mathbb{N})\Big];$

$\square$

$\texttt{NextIsGreater} :: \forall n \in \mathbb{N} \,.\, n < n+1$

$\texttt{Proof} \;=$

$(1) := \texttt{OverflowLemma}(n) : n+1 \notin n,$

$(2) := \texttt{SelfContainment}(n+1) : n+1 \in n+1,$

$(3) := \texttt{IneqSets}(1)(2)I(\#, \to)(\texttt{primPart}) : n \neq_{\mathbb{N}} n+1,$

$(4) := \texttt{HasOne}^2(n+1)(n)\eth\texttt{intersect}(n, n+1) : 1 \in n \cap n+1,$

$\texttt{Assume}\; m : n \cap n+1,$

$\texttt{Assume}\; (5) : m \neq n,$

$(6) := \texttt{FiniteInductionIsWellDefined}(n+1, m, (5)) : m+1 \in n,$

$(7) := \eth\texttt{primPart}(n+1)(m) : m+1 \in n+1,$

$() := \eth\texttt{intersect}(n, n+1)(7, 8) : m+1 \in n \cap n+1;$

$\rightsquigarrow (5) := I(\Rightarrow)I(\forall) : \forall m \in n \cap n+1 \,.\, m \neq n \Rightarrow m+1 \in n \cap n+1,$

$(4) := \eth\texttt{LinearlyInductive}(n)(4, 5) : n = n \cap n+1,$

$(5) := \texttt{IntersectSubset}(4) : n \subset n+1,$

$(6) := \eth\texttt{NaturalOrder}(5) : n \leq n+1,$

$(*) := \eth\texttt{StrictLess}(3, 5) : n < n+1;$

$\square$

$\texttt{after} :: \mathbb{N} \to ?\mathbb{N}$

$\texttt{after}\,(n) := \{m \in \mathbb{N} \,.\, m > n\}$

$\texttt{AfterDisjoint} :: \forall n \in \mathbb{N} \,.\, n \cap \texttt{after}(n) = \emptyset$

$\texttt{Proof} \;=$

$\texttt{Assume}\; m : n,$

$\texttt{Assume}\; (1) : m = n,$

$() := \eth\texttt{after}(n)\eth\texttt{StrictlyGreater}(1) : m \notin \texttt{after}(n);$

$\rightsquigarrow (1) := I(\Rightarrow) : m = n \Rightarrow m \notin \texttt{after}(n),$

$\texttt{Assume}\; (0) : m \neq n,$

$(2) := \texttt{FiniteInductionIsWellDefined}(n, m)(0) : m+1 \in n,$

$(3) := \texttt{OverflowLemma}(m) : m+1 \notin m,$

$(4) := \eth\texttt{NaturalOrder}(2, 3) : n \not\leq m,$

$() := \eth\texttt{after}(n)(4) : m \notin \texttt{after}(n);$

$\rightsquigarrow (5) := I(\Rightarrow) : m \neq n \Rightarrow m \notin \texttt{after}(n),$

$() := \texttt{EqAlternative}(m, n)E(|)(5, 4) : m \notin \texttt{after}(n);$

$\rightsquigarrow (*) := \eth\texttt{intersct}(n, \texttt{after}(n)) : n \cap \texttt{after}(n) = \emptyset;$

$\square$

$\texttt{NaturalShift} :: \forall n \in \mathbb{N} \,.\, (\texttt{after}(n), n+1, \sigma) : \texttt{NaturalSet}$

$\texttt{Proof} \; =$

$\texttt{Assume } m : \texttt{after}(n),$

$\texttt{Assume } (1) : n+1 = m+1,$

$(2) := \eth\texttt{NaturalSet}(1) : n = m,$

$(4) := \eth\texttt{after}(n)\eth\texttt{SrictlyGreater}(2) : m \notin \texttt{after}(n),$

$() := (4)(m) : \bot;$

$\rightsquigarrow (1) := E(\bot)I(\forall) : \forall m \in \texttt{after}(n) \,.\, m+1 \neq n+1,$

$\texttt{Assume } P :?\texttt{after}(n),$

$\texttt{Assume } (2) : n+1 \in P,$

$\texttt{Assume } (3) : \forall m \in P \,.\, m+1 \in P,$

$P' := n \cup P :?\mathbb{N},$

$(4) := \eth P'\eth\texttt{union}(n,P)\texttt{HasFirst}(n) : 1 \in P',$

$\texttt{Assume } m : P',$

$\texttt{Assume } (5) : m \in n,$

$\texttt{Assume } (6) : m \neq n,$

$(7) := \texttt{FiniteInductionIsWellDefined} : m+1 \in n,$

$(8) := \eth P'\eth\texttt{union}(n,P)(7) : m+1 \in P';$

$\rightsquigarrow (6) := I(\forall) : m \neq n \to m+1 \in P',$

$\texttt{Assume } (7) : m = n,$

$(8) := (7)(2) : m+1 \in P',$

$\rightsquigarrow (7) := I(\Rightarrow) : m = n \Rightarrow m+1 \in P',$

$() := \texttt{AllButOne}(n,n)E(|)(6,7)\eth P'\texttt{union}(n,P) : m+1 \in P';$

$\rightsquigarrow (5) := I(\Rightarrow) : m \in n \Rightarrow n \in P',$

$\texttt{Assume } (6) : m \in P',$

$() := (3)(6)\eth P'\texttt{union}(n,P) : m+1 \in P';$

$\rightsquigarrow (6) := I(\Rightarrow) : m \in P \to m+1 \in P',$

$() := \eth P'\eth\texttt{union}E(|)(5)(6) : m+1 \in n;$

$\rightsquigarrow (5) := I(\forall) : \forall m \in P' \,.\, m+1 \in P',$

$(6) := \eth\texttt{NaturalSet}(\mathbb{N})(4,5) : P' = \mathbb{N},$

$(7) := \texttt{AfterDisjoint} : n \cap \texttt{after}(n) = \emptyset,$

$(*) := (6)\texttt{DisjointCompletion}(n, \texttt{after}(n), P)(7) : P = \texttt{after}(n);$

$\rightsquigarrow (n) := I(\Rightarrow)I(\forall)\eth^{-1}\texttt{NaturalSet} : \Big[(\texttt{after}(n), n+1, \sigma) : \texttt{NaturalSet}\Big],$

$\square$

$\texttt{StructureOfNat3} :: \forall n \in \mathbb{N} \,.\, \mathbb{N} = n \sqcup \texttt{after}(n)$

$\texttt{Proof} \; =$

$\square$

$\texttt{ShiftReflectsOrder} :: \forall n \in \mathbb{N} \,.\, \forall m \in \texttt{after}(n) \,.\, n+1 \leq_{\mathbb{N}} m$

$\texttt{Proof} \ =$

$P := \{m \in \texttt{after}(n) \,.\, n+1 \leq_{\texttt{after}(n)} m \Rightarrow n+1 \leq_{\mathbb{N}} m\} :?\texttt{after}(n),$

$(1) := \eth\texttt{Reflexive}(\texttt{NaturalOrder})\eth P : n+1 \in P,$

$\texttt{Assume}\ m : P,$

$(2) := \texttt{NextIsGreater}(\mathbb{N})(m) : m <_{\mathbb{N}} m+1,$

$(3) := \texttt{FirstIsLowerBound}(\texttt{after}(n))(m) : n+1 \leq m,$

$(4) := \eth P(4) : n+1 \leq_{\mathbb{N}} m,$

$() := (2)(4) : n+1 \leq m+1;$

$\rightsquigarrow (2) := I(\forall)\eth P : \forall m \in P \,.\, m+1 \in P,$

$(3) := \eth\texttt{NaturalSet}(\texttt{after}(n))(1)(2) : P = \texttt{after}(n);$

$\square$

$\texttt{NaturalOrderIsTotal} :: \texttt{NaturalOrder} : \texttt{Total}$

$\texttt{Proof} \ =$

$P := \{n \in \mathbb{N} : \forall m \in \mathbb{N} \,.\, n \leq m | m \leq n\} :?\mathbb{N},$

$(1) := \texttt{FirstIsLowerBound}\eth\texttt{LowerBound}(Nat)\eth P : 1 \in P,$

$\texttt{Assume}\ n : P,$

$(2) := \texttt{StructureOfNat3}(n)\eth P : n = \{m \in \mathbb{N} : m \leq n\},$

$(3) := \texttt{NextIsGreater}(n) : n < n+1,$

$\texttt{Assume}\ m : \mathbb{N},$

$\texttt{Assume}\ (4) : m \in n,$

$() := (2)(3) : m < n+1;$

$\rightsquigarrow (4) := I(|)I(\Rightarrow) : m \in n \Rightarrow n+1 \leq m | m \leq n+1,$

$\texttt{Assume}\ m : \texttt{after}(n),$

$(5) := \texttt{NaturalShift}(n)\texttt{FirstIsLowerBound} : [n+1 : \texttt{LowerBound}(\texttt{after}(n))],$

$() := \eth\texttt{LowerBound}(n+1)(m)\texttt{ShiftReflectsOrder}(n) : m \leq n+1;$

$\rightsquigarrow (5) := I(|)I(\Rightarrow) : m \in \texttt{after}(n) \Rightarrow n+1 \leq m | m \leq n+1,$

$() := \texttt{StructureOfNat3}E(|)(4,5) : n+1 \leq m | m \leq n+1;$

$\rightsquigarrow (2) := I(\forall)\eth P I(\forall) : \forall n \in P \,.\, n+1 \in P,$

$(3) := \eth\texttt{NaturalSet}((1),(2)) : P = \mathbb{N},$

$(*) := \eth^{-1}\texttt{Total}(3) : \Big[\texttt{NaturalOrder} : \texttt{Total}\Big];$

$\square$

$\texttt{NextRespectsOrder} :: \forall a, b \in \mathbb{N} \,.\, a \leq b \iff a+1 \leq b+1$

$\texttt{Proof} \;=$

$\texttt{Assume}\ (1) : a \leq b,$

$\texttt{Assume}\ (2) : a = b,$

$(3) := I(=,\rightarrow)(\sigma)(2) : a+1 = b+1,$

$() := \eth^{-1}\texttt{ReflexiveNaturalOrder}(\mathbb{N})(3) : a+1 \leq b+1;$

$\leadsto (2) := I(\Rightarrow) : a = b \Rightarrow a+1 \leq b+1,$

$\texttt{Assume}\ (3) : a < b,$

$(4) := \texttt{NextIsGreater}(b) : b < b+1,$

$(5) := \texttt{FirstIsLowerBound}\eth^{-1}\texttt{after}(a)((3), b) : a+1 \leq b,$

$() := (4)(5) : a+1 < b+1;$

$\leadsto (3) := I(\Rightarrow) : a < b \Rightarrow a+1 \leq b+1,$

$() := \texttt{Dichtotmy}(1)E(|)((2),(3)) : a+1 \leq b+1;$

$\leadsto (1) := I(\Rightarrow) : a \leq b \Rightarrow a+1 \leq b+1,$

$\texttt{Assume}\ (2) : a+1 \leq b+1,$

$\texttt{Assume}\ (3) : a+1 = b+1,$

$(4) := \eth\texttt{NaturalSet}(\mathbb{N})(2) : a = b,$

$() := \eth^{-1}\texttt{ReflexiveNaturalOrder}(\mathbb{N}) : a+1 \leq b+1;$

$\leadsto (3) := I(\Rightarrow) : a+1 = b+1 \Rightarrow a \leq b,$

$\texttt{Assume}\ (4) : a+1 < b+1,$

$\texttt{Assume}\ (5) : a > b,$

$(6) := (1)(a,b)(7) : a+1 \leq b+1,$

$() := \texttt{Trichtomy}(\mathbb{N})(7)(8) : \perp;$

$\leadsto (7) := E(\perp) : a \leq b;$

$\leadsto (3) := I(\Rightarrow) : a+1 < b+1 \Rightarrow a \leq b,$

$() := \texttt{Dichtotmy}(1)E(|)((2),(3)) : a \leq b;$

$\leadsto (*) := I(\iff)(1)I(\Rightarrow) : a \leq b \iff a+1 \leq b+1;$

$\square$

$\texttt{NatIsWellOrdered} :: \mathbb{N} : \texttt{WellOrdered}$

$\texttt{Proof} \ =$

$\texttt{Assume}\ A : \texttt{HasNoMinimal}(\mathbb{N},$

$P := \{n \in \mathbb{N} : n < A\} :?\mathbb{N},$

$(1) := \texttt{FirstLowerBound}(\mathbb{N})(A) : 1 \leq A,$

$(2) := \eth\texttt{HasNoMinimal}(A)(1) : 1 < A,$

$(3) := \eth P(2) : 1 \in P,$

$\texttt{Assume}\ (4) : n \in P,$

$(5) := \eth P(n)\eth^{-1}\texttt{after}(n) : A \subset \texttt{after}(n),$

$(6) := \texttt{firstLowerBound}(\texttt{after}(n))(A)\texttt{ShiftReflectsOrder}(n) : n+1 \leq A,$

$(7) := \eth\texttt{HasNoMinimal}(A)(6) : n+1 < A,$

$() := \eth P(7) : n+1 \in P;$

$\leadsto (4) := I(\forall) : \forall n \in P\ .\ n+1 \in \mathbb{N},$

$(5) := \eth\texttt{NaturalSet}((3),(4)) : P = \mathbb{N},$

$(6) := \eth P\eth\texttt{StrictlyLess}\eth^{-1}\texttt{DisjointDisjointSubset}(A,P)(5)\texttt{UiversalCompliment} : A \subset P^{\complement} = \emptyset,$

$() := \texttt{EmptySubset}(6) : A = \emptyset,$

$\leadsto (1) := I(\forall) : \forall A : \texttt{HasNoMinimal}(\mathbb{N})\ .\ A = \emptyset,$

$(*) := \eth^{-1}\texttt{WellOrdered}(1) : \texttt{This};$

$\square$

1.4 Natural Objects

$$\texttt{NaturalObject} :: \prod \mathcal{C} : \texttt{WithTerminal} \,.\, ?\sum X \in \mathcal{C} \,.\, 1_{\mathcal{C}} \xrightarrow{\mathcal{C}} X \times X \xrightarrow{\mathcal{C}}$$

$$(X, u, \sigma) : \texttt{NaturalObject} \iff \forall A \in \mathcal{C} \,.\, \forall I : 1_{\mathcal{C}} \xrightarrow{\mathcal{C}} A \,.\, \forall g : X \xrightarrow{\mathcal{C}} X \,.$$
$$.\, \exists! f : X \xrightarrow{\mathcal{C}} A \,.\, uf = I \;\&\; Ig = u\sigma f \;\&\; \sigma f = fg$$

G

1.5 More Inductions and Recursions

$\texttt{FullInduction} :: \forall N : \texttt{NaturalSet} \,.\, \forall A :?N \,.\, \forall (0) : 0 \in A \,.\, \forall (00) : \forall n \in P \,.\, n+1 \in A \,.\, P = N$

where

$P = \{n \in N : \forall k \in n \,.\, k \in A\}$

$\texttt{Proof} =$

. . .

$\square$

$\texttt{hardRecursion} :: \prod N : \texttt{NaturalSet} \,.\, \prod X : \mathsf{SET} \,.\, \Big(X \times \big((N \times X) \to X\big)\Big) \to N \to X$

$\texttt{hardRecutsion}\,((a, f)) = \texttt{rec2}(a, f) := \Big(\texttt{rec}\big((\sigma(1), a), \Lambda(n, x) \in N \times X \,.\, (\sigma(n), f(n, x))\big)\Big)_2$

2 Integers

2.1 Arithmetics with the Zero

$\mathbb{N} := (\mathbb{N}, 1, \sigma) : \texttt{NaturalSet};$

$\mathbb{Z}_+ := (\mathbb{Z}_+, 0, \sigma) : \texttt{NaturalSet};$

$\texttt{naturalEmbedding} :: \mathbb{N} \to \mathbb{Z}_+$
$\texttt{naturalEmbedding}() = \texttt{implicit} := \texttt{rec}(0+1, \sigma)$

$\texttt{add} :: \mathbb{Z}_+ \to \mathbb{Z}_+ \to \mathbb{Z}_+$
$\texttt{add}() = (+) := \texttt{rec}(\mathrm{id}, \texttt{compose}(\sigma))$

$\texttt{ZeroIsNeutral} :: 0 : \texttt{Neutral}(+)$
$\texttt{Proof} =$
$(1) := \eth\texttt{add}(0)\eth\mathrm{id} : \forall n \in \mathbb{Z}_+ \,.\, 0 + n = n,$
$P := \{n \in \mathbb{Z}_+ : n + 0 = 0\} :?\mathbb{Z}_+,$
$(2) := (1)(0) : 0 + 0 = 0,$
$(3) := \eth P(2) : 0 \in P,$
$\texttt{Assume}\ n : P,$
$(4) := \eth\texttt{add}(n+1)\eth P\eth^{-1} n + 1 : n + 1 + 0 = \sigma(n+0) = \sigma(n) = n + 1,$
$() := \eth P(4) : n + 1 \in P;$
$\rightsquigarrow (4) := I(\forall) : \forall n \in P \,.\, n + 1 \in P,$
$(5) := \eth\texttt{NaturalSet}(\mathbb{Z}_+)(4, 5) : P = \mathbb{Z}_+,$
$(*) := \eth^{-1}\texttt{Neutral}\Big((1), (5)\Big) : \Big[n : \texttt{Neutral}(+)\Big];$
$\square$

$\texttt{OneCommutes} :: \forall n, k \in \mathbb{Z}_+ \,.\, (+)(n)(+)(1)(k) = (+)(1)(+)(n)(k)$
$\texttt{Proof} =$
$P := \{n \in \mathbb{Z}_+ : \forall k \in \mathbb{N} \,.\, (n + (1 + k)) = (1 + (n + k))\} :?\mathbb{Z}_+,$
$\texttt{Assume}\ k : \mathbb{Z}_+,$
$() := \texttt{ZeroIsNeutral} : (+)(0)(+)(1)(k) = (+)(1)(k) = (+)(1)(+)(0)(k);$
$\rightsquigarrow (1) := \eth P I(\forall) : 0 \in P,$
$\texttt{Assume}\ n : P,$
$\texttt{Assume}\ k : \mathbb{N},$
$(2) := \eth^3\texttt{add} : (1 + n) + k = \sigma(n) + k = \sigma(n + k) = 1 + (n + k);$
$() := \eth\texttt{add}\eth n\eth P(2)\eth\texttt{add} :$
$\quad : \sigma(n) + (1 + k) = \sigma(n + (1 + k))\sigma(1 + (n + k)) = 1 + (1 + (n + k)) = 1 + ((1 + n) + k) = 1 + (\sigma(n) + k);$
$\rightsquigarrow (2) := I(\forall)\eth P I(\forall) : \forall n \in P \,.\, P + 1 \in n,$
$(*) := \eth\texttt{NaturalSet}((1), (2)) : P = \mathbb{Z}_+;$
$\square$

$\mathtt{NextIsAddition} :: \forall n \in \mathbb{Z}_+ \,.\, (+)(n)(1) = \sigma(n)$

$\mathtt{Proof} \ =$

$P := \{n \in \mathbb{Z}_0 : (+)(n)(1)\} :?\mathbb{Z}_+,$

$(1) := \eth\mathtt{add}(0)\eth\mathtt{naturalEmbedding}(1) : (+)(0)(1) = 1 = \sigma(0),$

$(2) := \eth P(1) : 0 \in P,$

$\mathtt{Assume}\ n : P,$

$() := \eth^{-1}\mathtt{add}(+)(1)\mathtt{OneCommutes}\eth n\eth P\eth\mathtt{add}(+)(1) :$

$\quad : (+)(\sigma(n))(1) = (+)(n)(+)(1)(1) = (+)(1)(+)(n)(1) = (+)(1)(\sigma(n)) = \sigma\sigma(n);$

$\rightsquigarrow (3) := I(\forall) : \forall n \in P \,.\, n+1 \in P,$

$(*) := \eth\mathtt{NaturalSet}(\mathbb{Z}_+) : \mathbb{Z}_+ = 0;$

$\square$

$\mathtt{NextIsAssoc} :: \forall n, m \in \mathbb{Z}_+ \,.\, (n+m)+1 = n+(m+1)$

$\mathtt{Proof} \ =$

$P := \{n \in \mathbb{Z}_+ : (n+m)+1 = n+(m+1)\} :?\mathbb{Z}_+,$

$\mathtt{Assume}\ m : \mathbb{Z}_+,$

$() := \mathtt{ZeroIsNeutral} : (0+m)+1 = m+1 = 0+(m+1);$

$\rightsquigarrow (1) := I(\forall)\eth P : 0 \in P,$

$\mathtt{Assume}\ k : P,$

$\mathtt{Assume}\ m : \mathbb{Z}_+,$

$() := \eth\mathtt{add}(k+1)\mathtt{NextIsAdd}\eth k\eth P\mathtt{NextIAdd}\eth\mathtt{add} :$

$\quad : ((k+1)+m)+1 = \sigma(k+m)+1 = ((k+m)+1)+1 = (k+(m+1))+1 = \sigma(k+(m+1)) = k+1+(m$

$\rightsquigarrow (2) := I(\forall)\eth P I(\forall) : \forall k \in P \,.\, k+1 \in P,$

$(*) := \eth\mathtt{NaturalSet}(\mathbb{Z}_0)\big((1),(2)\big) : P = \mathbb{Z}_0;$

$\square$

$\mathtt{AdditionIsAssoc} :: (+) : \mathtt{Associative}(\mathbb{Z}_+)$

$\mathtt{Proof} \ =$

$P := \{k : \forall n, m \in \mathbb{Z}_+ \,.\, (n+m)+k = n+(m+k)\} :?\mathbb{Z}_+,$

$\mathtt{Assume}\ n, m : \mathbb{N},$

$() := \mathtt{ZeroIsNeutral}^2(n+m)(m) : (n+m)+0 = n+m = n+(m+0);$

$\rightsquigarrow (1) := I(\forall) : \forall n, m \in \mathbb{Z}_+ \,.\, (n+m)+0 = n+(m+0),$

$(2) := \eth P(1) : 0 \in P,$

$\mathtt{Assume}\ k : P,$

$\mathtt{Assume}\ n, m : \mathbb{N},$

$() := \mathtt{NextIsAssoc}(n+m, k)\eth P(k)\mathtt{NextIsAssoc}(n, m+k)\mathtt{NextIsAddition}(m, k) :$

$\quad : (n+m)+(k+1) = ((n+m)+k)+1 = (n+(m+k))+1 = n+((m+k)+1) = n+(m+k+1);$

$\rightsquigarrow (3) := I(\forall) : \forall n, m \in \mathbb{Z}_+ \,.\, (n+m)+k+1 = n+(m+k+1),$

$() := \eth P(3) : k+1 \in P;$

$\rightsquigarrow (3) := I(\forall) : \forall k \in P \,.\, k+1 \in P,$

$() := \eth\mathtt{NaturalSet}(\mathbb{Z}_+) : P = \mathbb{Z}_+;$

$\square$

$\texttt{AdditionCommutes} :: (+) : \texttt{Commutative}(\mathbb{Z}_+)$

$\texttt{Proof} =$

$P := \{n \in \mathbb{Z}_+ : \forall m \in \mathbb{Z}_+ \,.\, n + m = m + n\} :?\mathbb{Z}_+,$

$(1) := \eth P\texttt{ZeroIsNeutral} : 0 \in P,$

$\texttt{Assume}\ n : P,$

$\texttt{Assume}\ m : \mathbb{Z}_0,$

$() := \eth\texttt{add}\eth n\eth P\texttt{OneCommute} : (n+1) + m = 1 + (n+m) = 1 + (m+n) = m + (n+1);$

$\rightsquigarrow (2) := I(\forall)\eth P I(\forall) : \forall n \in P \,.\, n + 1 \in P,$

$(3) := \eth\texttt{NatalSet}(\mathbb{Z}_+) : P = \mathbb{Z}_+;$

$\square$

$\texttt{NaturalNumbersFormMonoid} :: (\mathbb{Z}_+, +, 0) : \texttt{CommutativeMonoid}$

$\texttt{Proof} =$

$\ldots$

$\square$

$\texttt{mult} :: \mathbb{N} \to \mathbb{N} \to \mathbb{N}$

$\texttt{mult}\,() = (\cdot) := \texttt{rec}(\texttt{const}(0), \Lambda f : \mathbb{Z}_+ \to \mathbb{Z}_+ \,.\, \Lambda n \in \mathbb{Z}_+ \,.\, f(n) + n)$

$\texttt{ZeroMult} :: \forall n \in \mathbb{N} \,.\, 0n = n0 = 0$

$\texttt{Proof} =$

$\texttt{Assume}\ n : \mathbb{Z}_+,$

$() := \eth\texttt{mult}(0) : 0n = 0;$

$\rightsquigarrow (1) := I(\forall) : \forall n \in \mathbb{N} \,.\, 0n = 0,$

$P := \{n \in \mathbb{Z}_+ n0 = 0\} :?\mathbb{Z}_+,$

$(2) := ((1))(0) : 0 \in P,$

$\texttt{Assume}\ n : P,$

$() := \eth\texttt{mult}(n+1) : (n+1)0 = n0 + 0 = 0 + 0 = 0;$

$\rightsquigarrow (3) := I(\forall)\eth P : \forall n \in P \,.\, n + 1 \in P,$

$(*) := \eth\texttt{NaturalSet}(\mathbb{Z}_+)(P)(2,3) : P = \mathbb{Z}_+;$

$\square$

$\texttt{UnitIsNeutral} :: \forall n \in \mathbb{N} \,.\, 1n = n1 = n$

$\texttt{Proof} =$

$\texttt{Assume}\ n : \mathbb{Z}_+,$

$() := \eth\texttt{mult}(1)(n) : 1n = n;$

$\rightsquigarrow (1) := I(\forall) : \forall n \in \mathbb{N} \,.\, 1n = n,$

$P := \{n \in \mathbb{N} \,.\, n1 = n\} :?\mathbb{Z}_+,$

$(2) := \texttt{ZeroMult}\eth P : 1 \in P,$

$\texttt{Assume}\ n : P,$

$() := \eth\texttt{mult}\eth P\texttt{NextIsAddition} : (n+1)1 = n1 + 1 = n + 1;$

$\rightsquigarrow (3) := I(\forall)\eth P : \forall n \in P \,.\, n + 1 \in P,$

$(*) := \eth\texttt{NaturalSet}(\mathbb{Z}_+) : P = \mathbb{Z}_+;$

$\square$

$\texttt{MultDistributive} :: ((\cdot),(+)) : \texttt{Distributive}(\mathbb{Z}_+)$

$\texttt{Proof} =$

$P := \{n \in \mathbb{Z}_+ : \forall k, m \in \mathbb{Z}_+ \,.\, n(m+k) = (nm) + (nk)\} :? \mathbb{Z}_+,$

$\texttt{Assume}\ m, k : \mathbb{Z}_+,$

$() := \texttt{ZeroMult}^3\texttt{ZeroNeutral} : 0(m+k) = 0 = 0 + 0 = (0m) + (0k);$

$\rightsquigarrow (1) := \eth P I(\forall) : 0 \in P,$

$\texttt{Assume}\ n : P,$

$\texttt{Assume}\ k, m : \mathbb{Z}_+,$

$() := \eth\texttt{mult}(n+1)\eth P \eth n \eth\texttt{Commutative}(\mathbb{Z}_+)(+)(nk, m)\eth^{-2}\texttt{mult}(n+1) :$

$: (n+1)(m+k) = n(m+k) + (m+k) = nm + nk + m + k = nm + m + nk + k = (n+1)m + (n+1)k;$

$\rightsquigarrow (2) := I(\forall)PI(\forall) : \forall n\ P \,.\, n+1 \in P,$

$(*) := \eth\texttt{NaturalSet}(\mathbb{Z}_+)(P)((1),(2)) : P = \mathbb{Z}_+;$

$\square$

$\texttt{BackMult} :: \forall n, m \in \mathbb{Z}_+ \,.\, n(m+1) = nm + n$

$\texttt{Proof} =$

$(*) := \texttt{NextIsAddition}(n)\texttt{MultDistributive}(n, m, 1)\texttt{UnitIsNeutral} : n(m+1) = nm + n1 = nm + n;$

$\square$

$\texttt{MultCommutes} :: (\cdot) : \texttt{Commutative}(\mathbb{Z}_+)$

$\texttt{Proof} =$

$P := \{n \in \mathbb{Z}_+ : \forall m \in \mathbb{Z}_+ \,.\, nm = mn\} :? \mathbb{Z}_+,$

$(1) := \texttt{ZeroMult}\eth P : 0 \in O,$

$\texttt{Assume}\ n : P,$

$\texttt{Assume}\ m : \mathbb{Z}_+,$

$:= \eth\texttt{mult}(n+1)\eth P\texttt{BackMult} : (n+1)m = nm + m = mn + m = m(n+1);$

$\rightsquigarrow (2) := I(\forall)\eth P I(\forall) : \forall n \in P \,.\, n+1 \in P,$

$(*) := \eth\texttt{NaturalSet}(\mathbb{Z}_+)(P)((1),(2)) : P = \mathbb{Z}_+;$

$\square$

$\texttt{MultIsAssoc} :: (\cdot) : \texttt{Associative}(\mathbb{Z}_+)$

$\texttt{Proof} \ =$

$P := \{n \in \mathbb{Z}_+ \,.\, \forall m, k \in \mathbb{Z}_+ \,.\, (nm)k = n(mk)\} : \mathbb{Z}_+,$

$\texttt{Assume}\ m, k : \mathbb{Z}_+,$

$() := \texttt{ZeroMult}^3 : (0m)k = 0k = 0 = 0(mk);$

$\rightsquigarrow (1) := I^2(\forall)\eth P : 0 \in P,$

$\texttt{Assume}\ n : P,$

$Q := \{m \in \mathbb{Z}_+ \,.\, \forall k \in \mathbb{Z}_+ \,.\, ((n+1)m)k = (n+1)(mk)\} : \mathbb{Z}_+,$

$\texttt{Assume}\ k : \mathbb{Z}_+,$

$() := \texttt{ZeroMult}^4 : ((n+1)0)k = 0k = 0 = (n+1)(0) = (n+1)(0k);$

$\rightsquigarrow (2) := I(\forall\eth Q) : 0 \in Q,$

$\texttt{Assume}\ m : Q,$

$K := \{k \in \mathbb{Z}_+ : ((n+1)(m+1))k = (n+1)((m+1)k)\} : \mathbb{Z}_+,$

$(3) := \texttt{ZeroMult}^3 : ((n+1)(m+1))0 = 0 = (n+1)0 = (n+1)((m+1)0),$

$(4) := \eth K(3) : 0 \in K,$

$\texttt{Assume}\ k : K,$

$() := \texttt{BackMult}\eth K\eth k\texttt{MultDistributive}\eth k\texttt{BackMult} :$

$\quad : ((n+1)(m+1))(k+1) = ((n+1)(m+1))k + (n+1)(m+1) =$

$\quad = (n+1)((m+1)k) + (n+1)(m+1) = (n+1)((m+1)k + (m+1)) = (n+1)((m+1)(k+1));$

$\rightsquigarrow (5) := I(\forall : \forall k \in K \,.\, k+1 \in K,$

$(6) := \eth\texttt{NaturalSet}(\mathbb{Z}_+)(K)((4),(5)) : K = \mathbb{Z}_+,$

$() := \eth K\eth Q(m+1) : m+1 \in Q;$

$\rightsquigarrow (5) := I(\forall) : \forall m \in Q \,.\, m+1 \in Q,$

$(6) := \eth\texttt{NaturalSet}(\mathbb{Z}_+)(Q)((2),(5)) : Q = \mathbb{Z}_+,$

$(3) := \eth Q\eth P(n+1) : n+1 \in P;$

$(*) := \eth\texttt{NaturalSet}(\mathbb{Z}_+)(Q)((2),(5)) : P = \mathbb{Z}_+,$

$\square$

$\texttt{TotalAddition} :: \forall n \in \mathbb{Z}_+ \,.\, \forall m \in \texttt{after}(n) \,.\, \exists t \in \mathbb{Z}_+ \,.\, n + t = m$

$\texttt{Proof} \;=$

$P := \{n \in \mathbb{Z}_+ \,.\, \forall m \in \texttt{after}(n) \,.\, \exists t \in \mathbb{Z}_+ \,.\, n + t = m\} :?\mathbb{Z}_+,$

$\texttt{Assume}\ m : \texttt{after}(0),$

$() := \texttt{NeutralZero}(m) : 0 + m = m;$

$\rightsquigarrow (1) := \eth I(\forall) : 0 \in P,$

$\texttt{Assume}\ n : P,$

$\texttt{Assume}\ m : \texttt{after}(n+1),$

$(2) := \eth\texttt{after}(n+1)(m) : m > n + 1,$

$(3) := (2)\texttt{NextIsGreater}(n) : m > n,$

$(t, 4) := \eth P(n)(3) : \sum t \in \mathbb{Z}_+ \,.\, n + t = m,$

$\texttt{Assume}\ (5) : t = 0,$

$(6) := \texttt{NeutralZero}(n)(5) : m = n + t = n,$

$(7) := \eth\texttt{StrictlyGreater}(3) : m \neq n,$

$() := I(\bot) : \bot;$

$\rightsquigarrow (5) := E(\bot)(t = 0) : t \neq 0,$

$(6) := \texttt{StructureOfNat}(\mathbb{Z}_+)(5) : [t : \texttt{Succesor}(\mathbb{Z}_+)],$

$(s, 7) := \eth\texttt{Succesor}(\mathbb{Z}_+)(t) : \sum s \in \mathbb{Z}_+ \,.\, t = s + 1,$

$() := \texttt{NextIsAddition}(n)\eth\texttt{Associative}(\mathbb{Z}_+)(+)(7)(5) : (n+1) + s = n + (1 + s) = n + t = m;$

$\rightsquigarrow (2) := I(\forall)\eth P I(\forall) : \forall n \in P \,.\, n + 1 \in P,$

$(*) := \eth\texttt{NaturalSet}(\mathbb{Z}_+)(P)((1), (2) : \mathbb{Z}_+ = P;$

$\square$

$\texttt{PositiveAddition} :: \forall n \in \mathbb{N} \,.\, \forall m \in \mathbb{Z}_+ \,.\, m + n > m$

$\texttt{Proof} \;=$

$P := \{n \in \mathbb{N} : \forall m \in \mathbb{Z}_+ \,.\, m + n > m\} :?\mathbb{N},$

$\texttt{Assume}\ m : \mathbb{Z}_+,$

$() := \texttt{NextIsAdditionNextIsGreater} : m + 1 = \sigma(m) > m;$

$\rightsquigarrow (1) := I(\forall)\eth P : 1 \in P,$

$\texttt{Assume}\ n : P,$

$\texttt{Assume}\ m : \mathbb{Z}_+,$

$() := \texttt{NextIsAdditon}\eth\texttt{Commutative}(\mathbb{Z}_+)(+)(n, 1)\eth\texttt{Associative}(\mathbb{Z}_+)(+)(m, 1, n)\eth P(n)\texttt{NextIsGreater} :$
$\quad : m + (n + 1) = (m + 1) + n > m + 1 > m;$

$\rightsquigarrow (2) := I(\forall)\eth P I(\forall) : \forall n \in P \,.\, n + 1 \in P,$

$(*) := \eth\texttt{NaturalSet}(\mathbb{N})(P)((1), (2)) : P = \mathbb{Z}_+;$

$\square$

$\texttt{NonnegativeAddition} :: \forall n \in \mathbb{Z}_+ \,.\, \forall m \in \mathbb{Z}_+ \,.\, m + n > m$

$\texttt{Proof} \;=$

$\ldots$

$\square$

2.2 Negative Numbers

$$\texttt{Integers} :: \texttt{CommutativeMonoid}$$

$$\texttt{Integers}\,() = \mathbb{Z} := \frac{\mathbb{Z}_+ \times \mathbb{Z}_+}{\texttt{diag}(\mathbb{Z}_+ \times \mathbb{Z}_+)}$$

$$\texttt{asInteger} :: \mathbb{Z}_+ \to \mathbb{Z}$$

$$\texttt{asInteger}\,(n) = \texttt{implicit} := [n, 0]$$

$$\texttt{negative} :: \mathbb{Z}_+ \to \mathbb{Z}$$

$$\texttt{negative}\,(n) = -n := [0, n]$$

$$\texttt{negate} :: \mathbb{Z} \to \mathbb{Z}$$

$$\texttt{negate}\,([n, m]) = -[n, m] := [m, n]$$

$$\texttt{Natural} :: ?\mathbb{Z}$$

$$z : \texttt{Natural} \iff \exists n \in \mathbb{Z}_+ \,.\, z = n$$

$$\texttt{Negative} :: ?\mathbb{Z}$$

$$n : \texttt{Negative} \iff \exists n \in \mathbb{N} \,.\, z = -n$$

$$\texttt{AbeleanIntegers} :: (\mathbb{Z}, +) : \texttt{Abelean}$$

$\texttt{Proof}$ =

...

□

$$\texttt{groupOfIntegers} :: \texttt{Abelean}$$

$$\texttt{groupOfIntegers}\,(()) = \mathbb{Z} := (\mathbb{Z}, +)$$

$$\texttt{InverseNumbers} :: \forall a : \texttt{Natural} \,.\, -a = 0 | -a : \texttt{Negative}$$

$\texttt{Proof}$ =

...

□

$$\texttt{InverseNumbers2} :: \forall a : \texttt{Negative} \,.\, -a : \texttt{Natural}$$

$\texttt{Proof}$ =

□

$\texttt{IntStructure} :: \mathbb{Z} = \texttt{Natural} \sqcup \texttt{Negative}$

$\texttt{Proof} \ =$

$\texttt{Assume}\ z : \texttt{Natural}\ \&\ \texttt{Negative},$

$(1, n) := \eth\texttt{Natural} : \sum n \in \mathbb{Z}_+ \,.\, z = [n, 0],$

$(2, m) := \eth\texttt{Negative} : \sum m \in \mathbb{N} \,.\, z = [0, z],$

$(3, t, s) := \eth\texttt{Eq}(\mathbb{Z})((1)(2)) : \sum t, s \in \mathbb{Z}_+ : n + t = s\ \&\ m + s = t,$

$(4) := \texttt{NonnegativeAdd}(t, n)(3) : t \leq n + t = s,$

$(5) := \texttt{PositiveAdd}(s, m)(3) : s < s + m = t,$

$(5) := \texttt{StrictAntisimmetry}((4), (5)) : \bot;$

$\rightsquigarrow (1) := \eth\texttt{Empty}(\mathbb{Z}) : \texttt{Natural}\ \&\ \texttt{Negative} = \emptyset,$

$\texttt{Assume}\ [n, m] : \mathbb{Z},$

$\texttt{Assume}\ (2) : n = m,$

$(3) := \eth\mathbb{Z}(2) : [n, m] = 0,$

$(4) := \eth\texttt{Natural}(3) : \Big[[n, m] : \texttt{Natural}\Big],$

$(5) := I(|)(\texttt{Negative}) : \Big[[n, m] : \texttt{Negative}|\texttt{Natural}\Big];$

$\rightsquigarrow (2) := I(\Rightarrow) : n = m \Rightarrow [n, m] : \texttt{Negative}|\texttt{Natural},$

$\texttt{Assume}\ (3) : n \neq m,$

$(4) := \eth\texttt{Natural} : n < m | m < n,$

$\texttt{Assume}\ (5) : n < m,$

$(t, 6) := \texttt{TotalAddition}(5) : \sum t \in \mathbb{Z}_+ \,.\, n + t = m,$

$(7) := (6)\eth\mathbb{Z} : [n, m] = [n, n + t] = [0, t],$

$() := \eth^{-1}\texttt{Negative}(7) : \Big[(n, m) : \texttt{Negative}\Big];$

$\rightsquigarrow (5) := I(\Rightarrow) : n < m \Rightarrow [n, m] : \texttt{Negative}|\texttt{Natural},$

$\texttt{Assume}\ (6) : n > m,$

$(7, t) := \texttt{TotalAddition}(5) : \sum t \in \mathbb{Z}_+ \,.\, m + t = n,$

$(8) := (7)\eth\mathbb{Z} : [n, m] = [m + t, m] = [t, 0],$

$(9) := \eth^{-1}\texttt{Natural}(8) : \Big[[n, m] : \texttt{Natural}\Big];$

$\rightsquigarrow (6) := I(\Rightarrow)I(|) : n > m \Rightarrow [n, m] : \texttt{Negative}|\texttt{Natural},$

$(7) := E(|)((4), (5), (6)) : \Big[[n, m] : \texttt{Negative}|\texttt{Natural}\Big];$

$\rightsquigarrow (3) := I(\Rightarrow) : n \neq m \Rightarrow [n, m] : \texttt{Negative}|\texttt{Natural},$

$() := \texttt{LEM}(n, m)E(|)((2), (3)) : [n, m] \in \texttt{Negative} \sqcup \texttt{Natural};$

$\rightsquigarrow () := \eth^{-1}\texttt{Universe} : \mathbb{Z} = \texttt{Negative} \sqcup \texttt{Natural};$

$\square$

2.3 Order Structure

$\texttt{GreaterInt} :: ?(\mathbb{Z} \times \mathbb{Z})$
$(a,b) : \texttt{GreaterInt} \iff a \geq b \iff a - b : \texttt{Natural}$

$\texttt{GreaterIntReflexive} :: \texttt{GreaterInt} : \texttt{Reflexive}(\mathbb{Z})$
$\texttt{Proof} \ =$
$\texttt{Assume}\ a : \mathbb{Z},$
$() := \eth\texttt{Inverse}(a)\eth^{-1}\texttt{Natural} : a - a = 0 : \texttt{Natural};$
$\rightsquigarrow () := \eth^{-1}\texttt{Reflexive}I(\forall)\eth^{-1}\texttt{GreateInt} : [\texttt{GreaterInt} : \texttt{Reflexive}],$
$\square$

$\texttt{GreaterIntAntisymmetric} :: \texttt{GreaterInt} : \texttt{Antysymmetric}(\mathbb{Z})$
$\texttt{Proof} \ =$
$\texttt{Assume}\ a, b : \mathbb{Z},$
$\texttt{Assume}\ (1) : a \geq b,$
$\texttt{Assume}\ (2) : b \geq a,$
$(3) := \eth\texttt{GreaterInt}(1) : [a - b : \texttt{Natural}],$
$(4) := \eth\texttt{GreaterInt}(2) : [b - a : \texttt{Natural}],$
$(5) := \texttt{InverseNumbers}(3) : b - a = 0 | b - a : \texttt{Negative},$
$(6) := \texttt{StructureOfInt}(4,5) : b - a = 0,$
$(7) := \texttt{UniqueInverse}(6) : b = a;$
$\rightsquigarrow (8) := \eth^{-1}\texttt{Antisymmetric}I(\forall) : \texttt{This};$
$\square$

$\texttt{GreaterIntTransitive} :: \texttt{GreaterInt} : \texttt{Transive}(\mathbb{Z})$
$\texttt{Proof} \ =$
$\texttt{Assume}\ a, b, c : \mathbb{Z},$
$\texttt{Assume}\ (1) : a \geq b,$
$\texttt{Assume}\ (2) : b \geq c,$
$(3, n) := \eth\texttt{GreaterInt}(1) : \sum n \in \mathbb{Z}_+ \,.\, a - b = [0, n],$
$(4, m) := \eth\texttt{GreaterInt}(2) : \sum m \in \mathbb{Z}_+ \,.\, b - c = [0, m],$
$() := \eth\texttt{Inverse}(-b)(a-c)\eth\texttt{Associative}(\mathbb{Z})(+)(3)(4)\eth\mathbb{Z}\eth\texttt{Natural} :$
$\quad : a - c = a + (-b + b) - c = (a - b) + (b - c) = [0, n] + [0, m] = [0, n + m] : \texttt{Natural};$
$\rightsquigarrow (1) := \eth^{-1}\texttt{Transitive}I(\forall) : (*);$
$\square$

$\texttt{IntOrder} :: \texttt{GreaterInt} : \texttt{Order}(\mathbb{Z})$
$\texttt{Proof} \ =$
$\ldots$
$\square$

$\texttt{orderedInt} :: \texttt{Poset}$
$\texttt{orderedInt}\,() = \mathbb{Z} := (\mathbb{Z}, \texttt{GreaterInt})$

$\texttt{IntOrderIsTotal} :: \texttt{GreaterInt} : \texttt{Total}$

$\texttt{Proof} \ =$

$\texttt{Assume}\ a, b : \mathbb{Z},$

$(1) := \texttt{IntStructure}(a - b) : \Big[a - b : \texttt{Natural} | a - b : \texttt{Negative}\Big],$

$\texttt{Assume}\ (2) : [a - b : \texttt{Natural}],$

$() := \eth^{-1}\texttt{GreaterInt} : a \geq b;$

$\rightsquigarrow (2) := I(\Rightarrow)I(|) : a - b : \texttt{Natural} \Rightarrow a \geq b | b \geq a,$

$\texttt{Assume}\ (3) : [a - b : \texttt{Negative}],$

$(4) := \texttt{InverseNumbers}(2)(3) : [b - a : \texttt{Natural}],$

$() := \eth^{-1}\texttt{GreaterInt} : b \geq a;$

$\rightsquigarrow (3) := I(\rightarrow)I(|) : a - b : \texttt{Negative} \Rightarrow a \geq b | b \geq a,$

$() := E(|)((1), (2), (3)) : a \geq b | b \geq a;$

$\rightsquigarrow (*) := \eth^{-1}\texttt{Total} : \texttt{This};$

$\square$

$\texttt{NatOrdersAgrees} :: \forall n, m \in \mathbb{Z}_+ \,.\, n \geq_{\mathbb{Z}_+} m \iff n \geq_{\mathbb{Z}} m$

$\texttt{Proof} \ =$

$\texttt{Assume}\ (1) : n \geq_{\mathbb{Z}_+} m,$

$(2) := \eth\mathbb{Z}(n - m) : n - m = [n, m],$

$(t, 3) := \eth\texttt{TotalAddition}(1) : \sum t \in \mathbb{Z}_+ \,.\, n = m + t,$

$(4) := (2)(3)\eth\mathbb{Z}\eth^{-1}\texttt{Natural} : n - m = [m + t, m] = [t, 0] : \texttt{Natural},$

$() := \eth\texttt{GreaterInt} : n \geq_{\mathbb{Z}} m;$

$\rightsquigarrow (1) := I(\Rightarrow) : n \geq_{\mathbb{Z}_+} m \Rightarrow n \geq_{\mathbb{Z}} m,$

$(2) := \texttt{UroborousLemma}(1) : n \geq_{\mathbb{Z}} m \Rightarrow n \geq_{\mathbb{Z}_+} m,$

$(*) := I(\iff)((1)(2)) : \texttt{This};$

$\square$

$\texttt{AdditionRespectsOrder} :: \forall n, m, t \in \mathbb{Z} \,.\, \forall (0) : n \geq m \,.\, n + t \geq m + t$

$\texttt{Proof} \ =$

$(1) := \eth\texttt{Abelean}(\mathbb{Z}, +)\eth\texttt{Inverse}(t)\eth\texttt{GreaterInt}(0) : n + t - m - t = n - m : \texttt{Natural},$

$(*) := \eth^{-1}\texttt{GreaterInt}(1) : n + t \geq m + t;$

$\square$

$\texttt{PositiveAddition} :: \forall a \in \mathbb{Z} \,.\, \forall n \in \mathbb{N} \,.\, a + n > n$

$\texttt{Proof} \ =$

$\dots$

$\square$

$\texttt{NonnegativAddition} :: \forall a \in \mathbb{Z} \,.\, \forall n \in \mathbb{Z}_+ \,.\, a + n \geq n$

$\texttt{Proof} \ =$

$\dots$

$\square$

2.4 Algebraic Structure

$\texttt{multInt} :: \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}$

$\texttt{multInt}\,([a,b],[c,d]) = [a,b][c,d] := [ac+bd, ad+cd]$

$\texttt{Assume}\ [a,b],[c,d] : \mathbb{Z},$

$\texttt{Assume}\ s,t : \mathbb{Z}_+,$

$\texttt{WellDefined} := \eth\texttt{mult}\eth\texttt{Distributive}(\mathbb{Z}_+)(\cdot,+)\eth\ldots\eth^{-1}\texttt{mult} :$

$$: [a+t,b+t][c+s,d+s] = \Big[(a+t)(c+s)+(b+t)(d+s),(a+t)(d+s)+(b+t)(c+s)\Big] =$$

$$= \Big[ac+tc+as+bd+bs+dt+st, ad+as+td+ts+bc+bs+tc+ts\Big] =$$

$$= \Big[(ac+bd)+(tc+as+bs+dt+st),(ad+bc)+(tc+as+bd+tc+ts)\Big] = [ac+bd,ad+bc];$$

$\square$

$\texttt{MultiplicationDistributive} :: (\cdot) : \texttt{Distributive}(\mathbb{Z},+)$

$\texttt{Proof} =$

$\texttt{Assume}\ [a,b],[c,d],[e,f] : \mathbb{Z},$

$$(*) := \ldots : [a,b]\Big([c,d]+[e,f]\Big) = [a,b][c+e,d+f] =$$

$$= \Big[a(c+e)+b(d+f),a(d+f)+b(c+e)\Big] = \Big[ac+ae+bd+bf,ad+af+bc+be\Big] =$$

$$= [ac+bd,ad+bc]+[ae+bf,af+be] = [a,b][c,d]+[a,b][e,f];$$

$\texttt{MultiplicationCommutative} :: (\cdot) : \texttt{Commutative}(\mathbb{Z},+)$

$\texttt{Proof} =$

$\ldots$

$\square$

$\texttt{MultiplicationAssociative} :: (\cdot) : \texttt{Associative}(\mathbb{Z},+)$

$\texttt{Proof} =$

$\square$

$\texttt{OneMultNeutral} :: \forall a \in \mathbb{Z} 1a = A$

$\texttt{Proof} =$

$\texttt{Assume}\ [n,m] : \mathbb{Z},$

$(*) := \ldots : [1,0][n,m] = [n,m];$

$\square$

$\texttt{IntegerRing} :: (\mathbb{Z},+,\cdot) : \texttt{CommutativeRing}$

$\texttt{Proof} =$

$\ldots$

$\square$

$\texttt{MultPresevesNat} :: \forall n, m : \texttt{Natural} \,.\, nm : \texttt{Natural}$

$\texttt{Proof} \;=$

$(*) := \ldots : [n, 0][m, 0] = [nm, 0] : \texttt{Natural};$

$\square$

$\texttt{PositiveNat} :: \forall n : \texttt{Natural} \,.\, \forall a, b \in \mathbb{Z} \,.\, \forall (0) : a \geq b \,.\, na \geq nb$

$\texttt{Proof} \;=$

$(1) := \eth\texttt{IntegerOrder}(0) : a - b : \texttt{Natural},$

$(2) := \eth\texttt{Distributive}(\mathbb{Z}, +)(\cdot)(n, a, -b)\texttt{MulPreservesNat}(n, a - b)(1) : na - nb = n(a - b) : \texttt{Natural},$

$(*) := \eth^{-1}\texttt{IntegerOrder}(2) : na \geq nb;$

$\square$

$\texttt{IntegerOrderedRing} :: (\mathbb{Z}, +, \cdot) : \texttt{OrderedRing}$

$\texttt{Proof} \;=$

$\square$

$\texttt{NaturalNumbers} :: \mathbb{Z}_+ = \texttt{Natural}$

$\texttt{Proof} \;=$

$\square$

$\texttt{PositiveNumber} :: \mathbb{Z}_{++} =_{2^{\mathbb{Z}}} \mathbb{N}$

$\texttt{Proof} \;=$

$\square$

$\texttt{NegativeNumbers} :: \mathbb{Z}_{--} = \texttt{Negative}$

$\texttt{Proof} \;=$

$\square$

$\texttt{NonDecreasingMult} :: \forall a \in \mathbb{Z}_+ \,.\, \forall b \in \mathbb{Z}_{++} \,.\, a \leq ab$

$\texttt{Proof} \;=$

$(1) := \texttt{PositiveNumber}\;\texttt{FirstIsMinimal}(\mathbb{Z}_+ +) : 1 \leq b,$

$(*) := \texttt{PositiveNat}(a, 1, b)(1) : a \leq ab;$

$\square$

$\texttt{IncreasingMult} :: \forall a, b \in \mathbb{Z}_{++} \,.\, \forall (0) : b > 1 \,.\, ab > a$

$\texttt{Proof} \;=$

$(n, 1) := \eth\texttt{IntegerGreater}(0) : \sum n \in \mathbb{Z}_{++} \,.\, b = n + 1,$

$(*) := (1)(ab)\eth\texttt{Associative}(\mathbb{Z})(\cdot)(a, n, 1)\texttt{PositiveAdd}(a)\texttt{NonDecreasingMult}(a, n) ::$
$ab = a(n + 1) = an + a > an \geq a;$

$\square$

$\texttt{UnitInteger} :: ?\mathbb{Z}$

$\texttt{UnitIntrger}\left(\mathbb{S}^0\right) = \{-1, 1\} :=$

$\texttt{absVal} :: \mathbb{Z} \to \mathbb{Z}_+$

$\texttt{absVal}\,(z) = |z| := \max z\mathbb{S}^0$

$\texttt{pow} :: \mathbb{Z}_+ \to \mathbb{Z} \to \mathbb{Z}$

$\texttt{pow}\,() := \texttt{rec}(\texttt{const}(1), \Lambda f : \mathbb{Z} \to \mathbb{Z} \;.\; \Lambda n \in \mathbb{Z} \;.\; f(n)n)$

$\texttt{pow}\,(n, z) := z^n$

$\texttt{PowerOfOne} :: \forall n \in \mathbb{Z}_+ + \;.\; 1^n = 1$

$\texttt{Proof} =$

$\ldots$

$\square$

$\texttt{PowerOfZero} :: \forall n \in \mathbb{Z}_+ \;.\; 0^n = 0$

$\texttt{Proof} =$

$\ldots$

$\square$

$\texttt{Exponentiation} :: \forall a \in \mathbb{Z} \;.\; \forall n, m \in \mathbb{Z}_+ \;.\; a^{n+m} = a^n a^m$

$\texttt{Proof} =$

$P := \{m \in \mathbb{Z}_+ : \forall n \in \mathbb{Z}_+ \;.\; \forall a \in \mathbb{Z} a^{n+m} = a^n a\} :?\mathbb{Z}_+,$

$\texttt{Assume}\ a : \mathbb{Z},$

$\texttt{Assume}\ n : \mathbb{Z}_+,$

$() := \ldots : a^n = a^n \cdot 1 = a^n \cdot a^0;$

$\rightsquigarrow (2) := \eth P\ I(\forall) : 0 \in P,$

$\texttt{Assume}\ m : P,$

$\texttt{Assume}\ n : \mathbb{Z}_+,$

$\texttt{Assume}\ a : \mathbb{Z},$

$() := \eth\texttt{Abelean}(\mathbb{Z}, +)\eth P(m)\eth\texttt{pow}\eth\texttt{CommutativeRing}(\mathbb{Z}, +, \cdot)\eth^{-1}\texttt{pow} : a^{n+m+1} = a^{(n+1)+m} = a^{n+1}a^m = a^n a a^m =$

$\rightsquigarrow (3) := I(\forall)\eth P I(\forall) : \forall m \in P \;.\; m + 1 \in P,$

$\square$

$\texttt{SignGroup} :: (\mathbb{S}^0, \cdot) : \texttt{Abelean}$

$\texttt{Proof} =$

$\ldots$

$\square$

2.5 Divisibility

$\texttt{SignNumberDecomposition} :: \forall a \in \mathbb{Z} . \exists s \in \mathbb{S}^0 : \exists n \in \mathbb{Z}_+ . a = sn$
$\texttt{Proof} =$
$(0) := \texttt{IntStructure}(a) : a : \texttt{Natural} | a : \texttt{Negative},$
$\texttt{Assume } (1) : [a : \texttt{Natural}],$
$() := I(=)(a) : a = a;$
$\rightsquigarrow (1) := I(\Rightarrow) : [a : \texttt{Natural}] \Rightarrow \texttt{This}(1, a),$
$\texttt{Assume } (2) : [a : \texttt{Negative}],$
$(3) := \eth\texttt{Negative} : -a \in \mathbb{Z}_+,$
$() := \eth\texttt{Ring}(\mathbb{Z}_+)(3) : a = (-1)(-a);$
$\rightsquigarrow (2) := I(\Rightarrow) : [a : \texttt{Negative}] \Rightarrow \texttt{This}(-1, -a),$
$(*) := E(|)(0)((2), (3)) : \texttt{This};$
$\dots$
$\square$

$\texttt{NoZeroDivizors} :: \forall a, b \in \mathbb{Z} . \forall (0) : ab = 0 . a = 0 | b = 0$
$\texttt{Proof} =$
$(s, n, 1) := \texttt{SignNumberDecomposition}(a) : \sum s \in \mathbb{S}^0 . \sum n \in \mathbb{Z}_+ . a = sn,$
$(z, m, 2) := \texttt{SignNumberDecomposition}(b) : \sum z \in \mathbb{S}^0 . \sum m \in \mathbb{Z}_+ . b = zm,$
$(3) := (1)(2)(3) : 0 = ab = snzm = (sz)(nm);$
$(4) := \texttt{ZeroAbsValue}(3) : \Big|(sz)(nm)\Big| = 0,$
$(5) := \texttt{SignPreservesAbsValue}(4)\texttt{NonegativeMult}(m, n)\texttt{PositiveAbsValue} : nm = \Big|nm\Big| = 0,$
$(6) := \texttt{NonegativeMult}\eth n \eth m(5) : n = 0 | m = 0,$
$(*) := (1)(2)(6) : a = 0 | b = 0;$
$\square$

$\texttt{Divizors} :: \mathbb{Z} \to ?\mathbb{Z}$
$b : \texttt{Divisors} \iff \Lambda a \in \mathbb{Z} . \exists c \in \mathbb{Z} . a = bc$

$\texttt{UniqueDivizor} :: \forall a \in \mathbb{Z} . \forall b : \texttt{Divizor}(a) . \exists! c \in \mathbb{Z} . a = bc$
$\texttt{Proof} =$
$(c, 1) := \eth\texttt{Divisors}(a)(b) : \sum c \in \mathbb{Z} . a = bc,$
$\texttt{Assume } c' : \mathbb{Z},$
$\texttt{Assume } (2) : a = bc',$
$(3) := (2)(1) : bc = bc',$
$(4) := (3) - bc'\eth\texttt{Ring}(\mathbb{Z}) : 0 = b(c - c'),$
$(*) := \texttt{NoZeroDivizors}(4) : c = c';$
$\square$

$\texttt{division} :: \sum a \in \mathbb{Z} . \texttt{Divizors}(a) \to \texttt{Divizors}(a)$
$\texttt{division}\,(b) = \frac{a}{b} := \texttt{UniqueDivizors}(a, b)$

$\texttt{Divides} :: ?(\mathbb{Z} \times \mathbb{Z})$

$(a, b) : \texttt{Divides} \iff a|b \iff \texttt{Divizors}(a) \subset \texttt{Divizors}(b)$

$\texttt{DividesIsPreorder} :: \texttt{Divides} : \texttt{Preorder}(\mathbb{Z})$

$\texttt{Proof} =$

$\dots$

$\square$

$\texttt{DivisorDivides} :: \forall a \in \mathbb{Z} . \forall b \in \texttt{Divizors}(a) . b|a$

$\texttt{Proof} =$

$\dots$

$\square$

$\texttt{DividesOrder} :: \texttt{Divides} : \texttt{Order}(\mathbb{Z}_+)$

$\texttt{Proof} =$

$\texttt{Assume } n, m : \mathbb{Z}_+,$

$\texttt{Assume } (1) : n|m,$

$\texttt{Assume } (2) : m|n,$

$(a, b, 3) := \eth\texttt{Divides}(n, m) : \sum a, b \in \mathbb{Z} . am = n \ \& \ bn = m,$

$\texttt{Assume } (4) : m = 0,$

$(5) := \texttt{ZeroMult}(4)(3) : n = 0,$

$() := (4)(5) : m = 0;$

$\rightsquigarrow (4) := I(\Rightarrow) : m = 0|n = 0 \Rightarrow m = n,$

$\texttt{Assume } (5) : m, n \in \mathbb{Z}_{++},$

$(6) := (3)_1(3)_2 : m = abm,$

$(7) := \texttt{MultSign}(3)(5) : a, b \in \mathbb{Z}_{++},$

$(8) := \texttt{IncreasingMult}(6)(7) : ab = 1,$

$(10) := (9)\texttt{IncreasingMult}(7)(8)\texttt{FirstIsMinimal}(\mathbb{Z}_+ +) : a, b = 1,$

$() := \eth\texttt{Ring}(\mathbb{Z}, +, \cdot)(3)(10) : m = n;$

$\rightsquigarrow (4) := I(\Rightarrow) : m, n \in \mathbb{Z}_{++} \Rightarrow m = n,$

$() := \texttt{StructureOfNat}(\mathbb{Z}_+)(3, 4) : n = m;$

$\rightsquigarrow (1) := I(\forall)\eth^{-1}\texttt{Antisymmetric} : \Big[\texttt{Divides} : \texttt{Antisymmetric}(\mathbb{Z}_+)\Big],$

$(*) := \eth^{-1}\texttt{Order}(\texttt{DividesIsPreorde}, 1) : \Big[\texttt{Divides} : \texttt{Order}(\mathbb{Z}_+)\Big];$

$\square$

$\texttt{EucleadeanProperty} :: \forall a, b \in \mathbb{Z} . \forall (0) : b \neq 0 . |a| \leq |ab|$

$\texttt{Proof} =$

$\dots$

$\square$

$\texttt{DivizorsOfZero} :: \texttt{Divisors}(0) = \mathbb{Z}$

$\texttt{Proof} =$

$\dots$

$\square$

$\texttt{UnitDivizors} :: \forall s \in \mathbb{S}^0 \,.\, \texttt{Divizors}(s) = \mathbb{S}^0$

$\texttt{Proof} \;=$

$\ldots$

$\square$

$\texttt{ArchimedeanProperty} :: \forall a \in \mathbb{Z}_+ \,.\, \forall b \in \mathbb{Z}_{++} \,.\, \exists n \in \mathbb{Z}_{++} \,.\, nb > a$

$\texttt{Proof} \;=$

$P := \{a \in \mathbb{Z}_+ : \forall b \in \mathbb{Z}_{++} \,.\, \exists n \in \mathbb{Z}_{++} \,.\, ab > a :? \mathbb{Z}_+,$

$(1) := \eth\mathbb{Z}_{++} : \forall b \in \mathbb{Z}_{++} \,.\, b > 0,$

$(2) := \eth P(1) : 0 \in P;$

$\texttt{Assume}\; a : P,$

$\texttt{Assume}\; b : \mathbb{Z}_{++},$

$(n, 3) := \eth P(a)(b) : \sum n \in \mathbb{Z}_{++} \,.\, nb \geq a,$

$(4) := \texttt{FirstIsMinimal}(\mathbb{Z}_{++})(b) : b \geq 1,$

$(*) := \eth\texttt{Ring}(\mathbb{Z})(3)(4) : (n+1)b = nb + b \geq a + b \geq a + 1;$

$\rightsquigarrow (3) := I(\forall)\eth P I(\forall) I(\exists)(n+1) : \forall a \in P \,.\, a + 1 \in P,$

$(*) := \eth\texttt{NaturalSet}(\mathbb{Z}_+) : P = \mathbb{Z}_+;$

$\square$

$\texttt{divideWithReminder} :: \mathbb{Z}_+ \to \mathbb{Z}_+ + \to \mathbb{Z}_+$

$\texttt{divideWethReminder}\,(a, b) = \div(a, b) := \max\{n \in \mathbb{Z}_+ : nb \leq a\}$

$\texttt{reminder} :: \mathbb{Z}_+ \to \mathbb{Z}_{++} \to \mathbb{Z}_+$

$\texttt{reminder}\,(a, b) = \mathrm{rem}(a, b) := a - \div(a, b)$

$\texttt{eucledeanAlgorithm} :: \mathbb{Z}_+ \to \mathbb{Z}_+ \to \texttt{List}(\mathbb{Z}_+ \times \mathbb{Z}_{++} \times \mathbb{Z}_{++})$

$\texttt{eucledeanAlgorithm}\,(a, 0) = \texttt{EA}(a, 0) := []$

$\texttt{EA}(a, b) := \Big(\div(a, b), \mathrm{rem}(a, b), b\Big) : \texttt{EA}(b, \mathrm{rem}(a, b));$

$\texttt{greatestCommonDivisor} :: \mathbb{Z}_{++} \to \mathbb{Z}_{++} \to \mathbb{Z}_{++}$

$\texttt{greates1CommonDivisor}\,(a, b) = \gcd(a, b) := \max \texttt{Divizor}(a) \cap \texttt{Divizor}(b) \cap \mathbb{Z}_{++}$

$\texttt{DivizorIsLess} :: \forall a \in \mathbb{Z}_{++} \,.\, \texttt{Divizors} \cap \mathbb{Z}_{++} \leq a$

$\texttt{Proof} \;=$

$\ldots$

$\square$

$\texttt{SumDivisibile} :: \forall a, b, c, d \in \mathbb{Z} \,.\, \forall (0) : d|a \;\&\; d|c \,.\, \forall (00) : c = a + b \,.\, d|b$

$\texttt{Proof} \;=$

$(a', (1)) := \eth\texttt{Divisible}(0) : \sum a' \in \mathbb{Z} \,.\, a = a'd,$

$(c', (2)) := \eth\texttt{Divisible}(0) : \sum c' \in \mathbb{Z} \,.\, c = c'd,$

$(3) := (00)(1)(2) : c'd = a'd + b,$

$(3) := (3) - a'd\eth\texttt{Ring}(\mathbb{Z}) : b = c'd - a'd = (c' - a')d,$

$(*) := \eth^{-1}\texttt{Devisible}(3) : d|b;$

$\texttt{ReminderBounds} :: \forall a \in \mathbb{Z}_+ \,.\, \forall b \in \mathbb{Z}_{++} \,.\, \mathrm{rem}(a, b) < b$

$\texttt{Proof} \;=$

$r := \mathrm{rem}(a, b) : \mathbb{Z}_+,$

$(1) := \eth\,\mathrm{rem}(a, b)(r) : a = b \div (a, b) + r,$

$\texttt{Assume}\ (2) : r \geq b,$

$(k, 3) := \eth\texttt{IntGreater}(2) : \sum k \in \mathbb{Z}_+ \,.\, r = b + k,$

$(4) := \eth\texttt{Ring}(\mathbb{Z})(3)(1) : a = b \div (a, b) + b + k = b(\div(a, b) + 1) + k \geq b(\div(a, b) + 1),$

$(5) := \texttt{NextIsGreater}(\div(a, b)) : \div(a, b) + 1 > \div(a, b),$

$() := \eth \div (a, b)(4)(5) : \perp;$

$\rightsquigarrow (*) := E(\perp) : r < b;$

$\square$

$\texttt{DivisionDecrease} :: \forall n \in \mathbb{Z}_{++} \,.\, \forall m : \texttt{Divizor}(n) \,.\, \forall (0) : m \geq 2 \,.\, \frac{n}{m} < n$

$\texttt{Proof} \;=$

$(1) := \eth\texttt{divide}(n, m) : m\frac{n}{m} = n,$

$(*) := \texttt{IncreasingMult}(1) : \frac{n}{m} < n;$

2.6 Prime Decomposition

$\texttt{Prime} :: ?\mathbb{Z}_{++}$

$p : \texttt{Prime} \iff \#\texttt{Divizors}(p) \cap \mathbb{Z}_{++} = 2$

$\texttt{two} :: \mathbb{Z}$

$\texttt{two}\,() = 2 := 1 + 1$

$\texttt{TwoIsPrime} :: 2 : \texttt{Prime}$

$\texttt{Proof} =$

$\ldots$

$\square$

$\texttt{PrimeDivizorExists} :: \forall n \in \mathbb{Z}_{++} \,.\, \texttt{Prime} \cap \texttt{Divizor}(n) \neq \emptyset$

$\texttt{Proof} =$

$P := \{n \in \mathbb{Z}_{++} : \forall m \in \mathbb{Z}_{++} : 2 \leq m \leq n : \texttt{Prime} \cap \texttt{Divizor}(n) \neq \emptyset\} :?\mathbb{Z}_{++},$

$(1) := \texttt{TeoIsPrime}\eth\texttt{P} : 2 \in P,$

$\texttt{Assume}\ n : n \in P,$

$\texttt{Assume}\ (2) : \forall m \in \mathbb{Z}_{++} \,.\, \forall() : 2 \leq m < n + 1 \,.\, m \not| n,$

$(3) := \eth^{-1}\texttt{Prime}(2) : [n + 1 : \texttt{Prime}],$

$() := \eth\texttt{Divizor}(n + 1)^2(3) : \texttt{Divizor}(n + 1) \cap \texttt{Prime} \neq \emptyset;$

$\leadsto (2) := I(\Rightarrow) : \ldots \Rightarrow \ldots,$

$\texttt{Assume}\ m : \mathbb{Z}_{++},$

$\texttt{Assume}\ (3) : 2 \leq m < n + 1,$

$\texttt{Assume}\ (4) : m | n + 1,$

$(5) := \texttt{FirstIsMinimal}(\texttt{after}(m - 1))(3) : m \leq n,$

$(p, 6) := \eth P(n)(5) : \sum p : \texttt{Prime} \,.\, p | m,$

$() := (4)(6) : p | n + 1;$

$\leadsto (2) := \texttt{LEM}(\ldots)(2)I(\forall) : \forall n \in P \,.\, n + 1 \in P,$

$(*) := \texttt{FullInduction}(\texttt{after}(1))(1, 2) : \texttt{This};$

$\square$

$\texttt{primeFactorization} :: \mathbb{Z}_{++} \to \texttt{List}(\texttt{Prime})$

$\texttt{primeFactorization}\,(1) = \texttt{PF}(1) := []$

$$\texttt{PF}(n) := p : \texttt{PF}\left(\frac{n}{p}\right)$$

$\quad \texttt{where} \quad p = \min \texttt{Prime} \cap \texttt{Divizor}(n);$

$\texttt{EucleadeanAlgorithmTerminates} :: \forall a, b \in \mathbb{Z}_+ \,.\, \texttt{len EA}(a, b) < \infty$

$\texttt{Proof} \;=$

$P := b \in \mathbb{Z}_+ : \forall a \in \mathbb{Z}_+ \,.\, \forall t \in b \,.\, \texttt{len EA}(a, t) < \infty :?\mathbb{Z}_+,$

$\texttt{Assume}\ a : \mathbb{Z}_+,$

$(1) := \eth\texttt{EA}(a, 0) : \texttt{EA}(a, 0) = [],$

$() := (1)\eth\texttt{len}[]\texttt{EmptyIsFinite} : \eth\texttt{lenE}, \texttt{A}(a, 0) = 0 < \infty;$

$\rightsquigarrow (1) := I(\forall)\eth P : 0 \in P,$

$\texttt{Assume}\ b : P,$

$\texttt{Assume}\ a : \mathbb{Z}_+,$

$(2) := \eth\texttt{EA}(a, b+1) : \texttt{EA}(a, b+1) = (\div(a, b+1), \mathrm{rem}(a, b+1), b+1) : \texttt{EA}\Big(b+1, \mathrm{rem}(a, b+1)\Big),$

$r := \mathrm{rem}(a, b+1) : \mathbb{Z}_+,$

$(3) := \texttt{ReminderBounds}(a, b+1) : 0 \geq r < b+1,$

$(5) := \texttt{FirstIsMinimal}(\texttt{after}(r-1))(b) : r \leq b,$

$(6) := \eth P(b)(5) : \texttt{len EU}(b+1, r) < \infty,$

$() := \eth\texttt{len}(2)(6) : \texttt{EA}(a, b+1) < \infty;$

$\rightsquigarrow (2) := I(\forall) : \forall b \in P \,.\, b+1 \in P,$

$(*) := \texttt{FullInduction}(1)(2) : \mathbb{Z}_+ = P;$

$\square$

$\texttt{PrimeFactorizationTerminates} :: \forall a \in \mathbb{Z}_+ + \;.\, \texttt{len PF}(a) < \infty$

$\texttt{Proof} \;=$

$\ldots$

$\square$

$\texttt{primeFacotization2} :: \mathbb{Z}_{++} \to \prod n : \mathbb{Z}_+ \,.\, \texttt{Nondecreasing}(n, \texttt{Prime})$

$\texttt{primeFactorization2}\,(a) = \texttt{PF2}(a) := \texttt{listAsFunc PF}(a)$

$\texttt{primeFactorization3} :: \mathbb{Z}_{++} \to \prod n : \mathbb{Z}_+ \,.\, \texttt{Increasing}(n, \texttt{Prime})\ \&\ n \to \mathbb{Z}_{++}$

$\texttt{primeFactorization3}\,(a) = \texttt{PF3}(a) := \texttt{count PF}(a)$

$$\texttt{PrimeFactorization} :: \forall a \in \mathbb{Z}_{++} \,.\, a = \prod_{i=1}^{n} p_i \quad \texttt{where} \quad (n, p) = \texttt{PF2}(a)$$

$\texttt{Proof} \;=$

$\ldots$

$\square$

$$\texttt{PrimeFactorization2} :: \forall a \in \mathbb{Z}_{++} \,.\, a = \prod_{i=1}^{n} p_i^{k_i} \quad \texttt{where} \quad (n, p, k) = \texttt{PF3}(a)$$

$\texttt{Proof} \;=$

$\ldots$

$\square$

$\texttt{EucleadeanAlgorithmComputesGCD} :: \forall a, b \in \mathbb{Z}_{++} \ . \ \gcd(a,b) = (\texttt{head reverse EA}(a,b))_3$

$\texttt{Proof} \ =$

$(n, s, r, d) := \texttt{listAsFunc EA}(a,b) : \sum n \in \mathbb{N} \ . \ n \to \mathbb{Z}_+^2 \times \mathbb{Z}_{++},$

$\texttt{Assume} \ (1) : n = 1,$

$(2) := \eth(n,s,r,d)(1)\eth\texttt{EA}(a,b) : a = s_1 b,$

$(3) := \eth\gcd(a,b)(2) : \gcd(a,b) = b,$

$(4) := \eth(n,s,r,d)(3) : d_n = \gcd(a,b);$

$\leadsto (1) := I(\Rightarrow) : n = 1 \Rightarrow d_n = \gcd(a,b),$

$\texttt{Assume} \ (2) : n > 1,$

$(3) := \eth(n,s,r,d) :$

$\quad : \forall i \in (n-1) \ . \ d_i = d_{i+1}s_{i+1} + r_{i+1} \ \& \ d_{i+1} = r_i \ \& \ r_n = 0 \ \& \ a = d_1 s_1 + r_1 \ \& \ b = d_1,$

$(4) := \eth\texttt{Reflecive}(|)(d_n) : d_n | d_n,$

$(5) := \texttt{ZeroDivizors}(d_n) : d_n | 0,$

$\texttt{Assume} \ i : n,$

$\texttt{Assume} \ (6) : 1 < i < n,$

$\texttt{Assume} \ (7) : d_n | d_i \ \& \ d_n | r_i,$

$()_1 := (3)_1(i-1)\texttt{SummDivisible}(7) : d_n | d_{i-1},$

$()_2 := (3)_2(7) : d_n | r_{i-1};$

$\leadsto (6) := I(\forall)I(\forall)I(\Rightarrow) :$

$\quad : \forall i \in n \ . \ \forall()1 < i < n \ . \ d_n | d_i \ \& \ d_n | r_i \Rightarrow d_n | d_{i-1} \ \& \ d_n | r_{i-1},$

$(7) := \texttt{ReverseFiniteInduction}(n)((4),(5),(6)) : \forall i \in n \ . \ d_n | d_1 \ \& \ d_n | r_i,$

$(8) := (3)_1(1)(7)(1)(3)_4\eth\texttt{divides} : d_n | a \ \& \ d_n | b,$

$(9) := \eth\gcd(a,b)(8) : d_n | \gcd(a,b),$

$(10) := \texttt{SumDivisible}(3)_4(\gcd(a,b)) : \gcd(a,b) | r_1,$

$\texttt{Assume} \ i : n,$

$\texttt{Assume} \ (11) : 1 < i < n,$

$\texttt{Assume} \ (12) : \gcd(a,b) | d_i \ \& \ \gcd(a,b) | r_i,$

$()_1 := (3)_2(i)(12)_2 : \gcd(a,b) | r_{i+1};$

$()_2 := \texttt{SumDivisible}(3)_1(i)()_2 : \gcd(a,b) | d_{i+1};$

$\leadsto (11) := I(\forall)I(\forall)I(\Rightarrow) :$

$\quad : \forall i \in n \ . \ \forall() : 1 < i < n \ . \ \gcd(a,b) | d_i \ \& \ \gcd(a,b) | r_i \Rightarrow \gcd(a,b) | d_{i+1} \ \& \ \gcd(a,b) | r_{i+1},$

$(12) := \texttt{FiniteInduction}(n)((3)_5,(10),(1)) : \forall i \in n \ . \ \gcd(a,b) | d_i \ \& \ \gcd(a,b) | r_i,$

$(13) := (12)_1(n) : \gcd(a,b) | d_n,$

$() := \eth\texttt{Antisymmetric}(9)(13) : \gcd(a,b) = d_n;$

$\leadsto (*) := E(|)\texttt{StructureOfNat}(n)(1) : \gcd(a,b) = d_n,$

$\square$

$\texttt{BezuatIdentity} :: \forall a, b \in \mathbb{Z}_{++} \,.\, \forall z \in \mathbb{Z} \,.\, \exists u, v \in \mathbb{Z} \,.\, ua + vb = z \gcd(a, b)$

$\texttt{Proof} \;=$

$(n, s, r, d) := \texttt{EA}(a, b) : \sum n \in \mathbb{N} \,.\, n \to \mathbb{Z}_+^2 \times \mathbb{Z}_{++},$

$(1) := \eth(n, s, r, d) :$

$\quad : \forall i \in (n - 1) \,.\, d_i = d_{i+1} s_{i+1} + r_{i+1} \;\&\; d_{i+1} = r_i \;\&\; r_n = 0 \;\&\; a = d_1 s_1 + r_1 \;\&\; b = d_1,$

$I := \texttt{idealGen}(\mathbb{Z})(a, b) : \texttt{Ideal}(\mathbb{Z}),$

$(3) := \eth I(b, (1)_5) : d_1 \in I,$

$(4) := \eth\texttt{Ideal}(1)_4 \eth I(a) : r_1 \in I,$

$\texttt{Assume } i : n,$

$\texttt{Assume } (5) : 1 < i < n,$

$\texttt{Assume } (6) : r_i \in I \;\&\; d_i \in I,$

$()_1 := (1)_2(i)(6) : d_{i+1} \in I,$

$()_2 := \eth\texttt{Ideal}(1)_1(i)()_1(r_{i+1}) : r_{i+1} \in I;$

$\rightsquigarrow (5) := I(\forall) I(\forall) I(\Rightarrow) :$

$\quad : \forall i \in n \,.\, \forall() : 1 < i < n \,.\, d_i \in I \;\&\; r_i \in I \Rightarrow \gcd(a, b) | d_{i+1} \;\&\; \gcd(a, b) | r_{i+1},$

$(6) := \texttt{FiniteInduction}(n)(3, 4, 5) : \forall i \in n \,.\, d_i, r_i \in I,$

$(7) := (6)(n)\texttt{EuclideanAlgorithComputesGCD}(a, b) : \gcd(a, b) \in I,$

$(8) := \eth I(7) : \exists v, u \in \mathbb{Z} \,.\, va + ub = \gcd(a, b),$

$(*) := k(8) : kva + kub = \gcd(a, b);$

$\square$

$\texttt{EuclidsLemma} :: \forall a, b \in \mathbb{Z}_{++} \,.\, \forall p : \texttt{Prime} \,.\, \forall(0) p | ab \,.\, p | a \Big| p | b$

$\texttt{Proof} \;=$

$\texttt{Assume } (1) : \gcd(p, b) = 1,$

$(u, v, 2) := \texttt{BezautIdentity}(p, b, 1)(1) : \sum u, v \in \mathbb{Z} \,.\, ub + vp = 1,$

$(3) := a(2) : uab + vpb = 1,$

$() := \texttt{DividibleSum}(3)(0) : p | a;$

$\rightsquigarrow (1) := I(\Rightarrow) : \gcd(p, b) = 1 \Rightarrow p | a \Big| p | b,$

$\texttt{Assume } (2) : \gcd(p, b) \neq,$

$() := \eth\texttt{Prime}(p)(2)\eth^{-1}\texttt{Divisible} : p | b;$

$\rightsquigarrow (2) := I(\rightarrow) : \gcd(p, b) \neq 1 \Rightarrow p | a \Big| p | b,$

$(*) := E(|)\texttt{StructureOfNat}(\gcd(p, b))(1)(2) : p | a \Big| p | b;$

$\square$

$\texttt{IterattedEuclidsLemma} :: \forall n \in \mathbb{N} . \forall a : n \to \mathbb{Z}_{++} . \forall p : \texttt{Prime} . \forall (0) : p | \prod_{i=1}^{n} a . \exists i \in n : p | a_i$

$\texttt{Proof} =$

$P := \{n \in \mathbb{N} : \forall p : \texttt{Prime} . \forall a : n \to \mathbb{Z}_{++} . \forall () : p | \prod_{i=1}^{n} a . \exists i \in n : p | a_i\} :?\mathbb{N},$

$(1) := \eth P(1) : 1 \in P,$

$\texttt{Assume}\ n : P,$

$\texttt{Assume}\ a : n + 1 \to \mathbb{Z}_{++},$

$\texttt{Assume}\ p : \texttt{Prime},$

$\texttt{Assume}\ (0) : p | \prod_{i=1}^{n+1} a_i,$

$(2) := \texttt{EuclidsLemma}(0) : p | a_{n+1} \Big| p | \prod_{i=1}^{n} a_i,$

$() := \eth P(n)(2) : \exists i \in n + 1 . p | a_i;$

$\rightsquigarrow (2) := I(\forall)\eth P I^3(\forall) : \forall n \in P . n + 1 \in P,$

$(*) := \eth\texttt{NaturalSet}(\mathbb{N})\Big((1), (2)\Big) : \mathbb{N} = P;$

$\square$

$\texttt{length} :: \mathbb{Z}_{++} \to \mathbb{Z}_{+}$

$\texttt{length}\,(a) = L(a) := \texttt{len PD2}(a)$

$\texttt{Coprime} :: ?\mathbb{Z}_{++} \times \mathbb{Z}_{++}$

$a, b : \texttt{Coprime} \iff \gcd(a, b) = 1$

$\texttt{CoprimeSet} :: ??\mathbb{Z}_{++}$

$A : \texttt{CoprimeSet} \iff \forall a, b \in A . a \neq b \Rightarrow (a, b) : \texttt{Coprime}$

$\texttt{ChineseReminder} :: \forall A : \texttt{CoprimeSet}\ \&\ \texttt{Finite} . \forall n : \prod a \in A . (a - 1)_{\mathbb{Z}_+} .$

$\exists! N \in \prod_{a \in A} a : \forall a \in A .\ \mathrm{rem}(N, a) = n_a$

$\texttt{Proof} =$

$\dots$

$\square$

$\texttt{MainTheoremOfArithmetics} :: \forall a \in \mathbb{Z}_{++} . \forall n \in \mathbb{Z}_{+} . \forall p : \texttt{Nondecreasing}(n, \texttt{Prime})$

$. \forall (0) : a = \prod_{i=1}^{n} p_i . p = \texttt{PD2}(a)$

$\texttt{Proof} =$

$P := \{l \in \mathbb{Z}_{+} : \forall a \in \mathbb{Z}_{++} . L(a) = l \Rightarrow \texttt{This}(a)\} :?\mathbb{Z}_{+}+,$

$\texttt{Assume}\ a : \mathbb{Z}_{++},$

$\texttt{Assume}\ (1) : L(a) = 0,$

$(2) := \eth L(a)(1) : a = 1,$

$\texttt{Assume}\ n : \mathbb{Z}_{+},$

$\texttt{Assume}\ p : \texttt{Nondecreasing}(n, \texttt{Prime}),$

Assume $(3) : a = \prod_{i=1}^{n} p_i$,

Assume $(4) : n \neq 0$,

$(5) :=$ (2)ð`Divides`$(3)(p_1) : p_1|1$,

$(6) :=$ `UnitDivizors`$(5) : p_1 \in \mathbb{S}^0$,

$() :=$ `UnitDivizors`(6)ð`Prime`$(p_1) : \perp$;

$\rightsquigarrow (4) := E(\perp) : n = 0$,

$() :=$ (2)ð`PF2`(1)(4)ð`emptyFunc` $: p =$ `PF2`(a);

$\rightsquigarrow (1) :=$ ð$P : 0 \in P$,

Assume $l : P$,

Assume $a : \mathbb{Z}_{++}$,

Assume $(2) : L(a) = l + 1$,

$q :=$ `PF2`$(a)_2$: `Nondecreasing`$(l+1,$ `Prime`$)$,

Assume $n : \mathbb{Z}_+$,

Assume p : `Nondecreasing`$(n,$ `Prime`$)$,

Assume $(3) : a = \prod_{i=1}^{n} p_i$,

$(4) :=$ `PrimeFactorization`$(a) : a = \prod_{i=1}^{l+1} q_i$,

$(5) :=$ ð`divides`$(3)(4)(q_1) : q_1 | \prod_{i=1}^{n} p_i$,

$(i, 6) :=$ `IteratedEuclidsLemma`$(5) : \sum i \in n \,.\, q_1|p_i$,

$(7) :=$ ð^2`Prime`$(q_1, p_i)(6) : q_1 = p_i$,

$(8) :=$ ð`divides`$(4)(3)(p_1) : p_1 | \prod_{i=1}^{l+1} q_i$,

$(j, 9) :=$ `IteratedEuclidsLemma`85$) : \sum j \in l + 1 \,.\, p_1|q_j$,

$(10) :=$ ð^2`Prime`$(q_j, p_1)(9) : q_1 = p_i$,

$(11) :=$ ð^2`Nondecreasing`$(p, q) : p_i = q_1 \leq q_j = p_1 \leq p_i \;\&\; q_j = p_1 \leq p_i = q_1 \leq p_j$,

$(12) :=$ `DoubleIneq`$(10, 11) : i = 1 = j$,

$(13) :=$ ð$L\left(\frac{a}{q_1}\right) : L\left(\frac{a}{q_1}\right) = l$,

$(14) := \frac{(3)}{q_1}(12) : \frac{a}{q_1} = \prod_{i=2}^{n} p_i$,

$(15) :=$ ð$P(l)(13)(14) : l = n - 1 \;\&\; q_{+1} = p_{+1}$,

$() :=$ (2)ð$q(15)(12)$: `PF2`$(a) = (l + 1, q) = (n, p)$;

$\rightsquigarrow (2) :=$ ð$P : \forall l \in P \,.\, l + 1 \in P$,

$(*) :=$ ð`NaturalSet`$(\mathbb{Z}_+)(P)(1, 2) : P = \mathbb{Z}_+$;

$\square$

2.7 Factorial Function

$\texttt{factorial} :: \mathbb{Z}_+ \to \mathbb{Z}_{++}$

$\texttt{factorial}\,(n) = n! := \texttt{rec2}(1, \Lambda(n, f) \in \mathbb{Z}_+ \times \mathbb{Z}_{++} \,.\, nf)$

$\texttt{factorialIsDivisible} :: \forall n \in \mathbb{Z}_{++} \,.\, \forall k \in n \,.\, k | n!$

$\texttt{Proof} \ =$

$\ldots$

$\square$

3 Rational Numbers

3.1 The Field of Fractions

$\texttt{MultPart} :: \texttt{IntegralDomain} \to \mathsf{SET}$
$\texttt{MultPart}(Z) = Z^{\times} := Z \setminus \{0\}$

$\texttt{FieldOfFrac} :: \texttt{IntegralDomain} \to \mathsf{SET}$

$$\texttt{FieldOfFrac}(Z) = \mathrm{Frac}(Z) := \frac{Z \times Z^{\times}}{\Big\{\big((a,b),(c,d)\big) | a, c \in Z; b, d \in Z^{\times} : ad = cb\Big\}}$$

$R := \{\big((a,b)),(c,d)\big) | a, c \in Z; b, d \in Z^{*} : ad = bc\Big\} :?(Z \times Z^{\times}),$
$\texttt{Assume}\ (a,b) : Z \times Z^{*},$
$(1) := I(+)(ab) : ab = ab,$
$(2) := \eth R(1) : (a,b) \in R;$
$\rightsquigarrow (1) := I(\forall)\eth^{-1}\texttt{Reflexive}(R) : [R : \texttt{Reflexive}(Z \times Z^{\times})],$
$\texttt{Assume}\ \Big((a,b),(c,d)\Big) : R,$
$(2) := \eth R\Big((a,b),(c,d)\Big) : ad = cb,$
$(3) := Q(=)(2) : bc = cb,$
$() := \eth R(3) : \Big((c,d),(a,b)\Big) \in R;$
$\rightsquigarrow (2) := I(\forall) I\texttt{Symmetric} : [R : \texttt{Symmetric}(Z \times Z^{\times})],$
$\texttt{Assume}\ (a,b),(c,d),(f,g) : Z \times Z^{*},$
$\texttt{Assume}\ (3) : \Big((a,b),(c,d)\Big), \Big((a,b),(c,d)\Big) \in R,$
$(4) := \eth R\Big((a,b),(c,d)\Big) : ad = cb,$
$(5) := \eth R\Big((c,d),(f,g)\Big) : cg = fd,$
$(6) := (4)g : adg = cbg,$
$(7) := (5)b : cbg = fdb,$
$(8) := (6)(7) : adg = fdb,$
$(9) := (8) - fdb\eth\texttt{CommutativeRing}(Z) : 0 = adg - fdb = d(ag - fb),$
$(10) := \eth\texttt{IntegralDomain}(Z)(9) : ag = fb,$
$() := \eth R(10) : \Big((a,b),(g,f)\Big) \in R;$
$\rightsquigarrow (3) := \eth^{-1}\texttt{Transitive} : [R : \texttt{Transitive}(Z \times Z^{\times})],$
$(4) := \eth^{-1}(\texttt{Equivalence}) : [R : \texttt{Equivalence}(Z \times Z^{\times})];$
$\square$

$\texttt{fraction} :: \prod Z : \texttt{IntegralDomain} \,.\, Z \times Z^{\times} \to \mathrm{Frac}(Z)$

$\texttt{fraction}\,(a, b) = \dfrac{a}{b} := [a, b]$

$\texttt{fracMult} :: \prod Z : \texttt{IntegralDomain} \,.\, \mathrm{Frac}(Z) \to \mathrm{Frac}(Z) \to \mathrm{Frac}(Z)$

$\texttt{fracMult}\left(\dfrac{a}{b}, \dfrac{c}{d}\right) = \dfrac{a}{b}\dfrac{c}{d} := \dfrac{ac}{bd}$

$\texttt{Assume}\ n, m : Z^{\times},$

$(*) := \eth\texttt{fracMult}\eth\texttt{CommutativeRing}(Z)\eth\,\mathrm{Frac}(Z)\eth^{-1}\texttt{fracMult} :$

$$: \frac{na}{nb}\frac{mc}{md} = \frac{namc}{nbmd} = \frac{nmac}{nmbd} = \frac{ac}{bd} = \frac{a}{c}\frac{b}{d};$$

$\square$

$\texttt{fracAdd} :: \prod Z : \texttt{IntegralDomain} \,.\, \mathrm{Frac}(Z) \to \mathrm{Frac}(Z) \to \mathrm{Frac}(Z)$

$\texttt{fracAdd}\left(\dfrac{a}{b}, \dfrac{c}{d}\right) = \dfrac{a}{b} + \dfrac{c}{d} := \dfrac{ad + cb}{bd}$

$\texttt{Assume}\ n, m : Z^{\times},$

$(*) := \eth\texttt{fracAdd}\eth\texttt{CommutativeRing}(Z)\eth\,\mathrm{Frac}(Z)\eth^{-1}\texttt{FracAdd} :$

$$: \frac{na}{nb} + \frac{mc}{md} = \frac{namd + mcnb}{nbmd} = \frac{nm(ad + cb)}{nmbd} = \frac{ad + cb}{bd} = \frac{a}{b} + \frac{c}{d};$$

$\texttt{FracAddAssoc} :: \forall Z : \texttt{IntegralDomain} \,.\, \texttt{fracAdd}(Z) : \texttt{Associative}\Big(\mathrm{Frac}(Z)\Big)$

$\texttt{Proof} =$

$\texttt{Assume}\ \dfrac{a}{b}, \dfrac{c}{d}, \dfrac{f}{g} : \mathrm{Frac}(Z),$

$(*) := \eth^2\texttt{fracAdd}\eth\texttt{CommutativeRing}(Z)\eth^{-2}\texttt{fracAdd} :$

$$: \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{f}{g} = \frac{ad + cb}{bd} + \frac{f}{g} = \frac{(ad + cb)g + fbd}{bdg} = \frac{adg + cbg + fbd}{bdg} =$$

$$= \frac{adg + b(cg + fd)}{bdg} = \frac{a}{b} + \frac{cg + fd}{dg} = \frac{a}{b} + \left(\frac{c}{d} + \frac{f}{g}\right);$$

$\square$

$\texttt{FracAddCommute} :: \forall Z : \texttt{IntergralDomain} \,.\, \texttt{fracAdd}(Z) : \texttt{Commutative}\Big(\mathrm{Frac}(Z)\Big)$

$\texttt{Proof} =$

...

$\square$

$\texttt{FracAddNeutral} :: \forall Z : \texttt{IntegralDomain} \,.\, \forall n \in Z^{\times} \,.\, \dfrac{0}{n} : \texttt{Neutral}\Big(\mathrm{Frac}(Z), +\Big)$

$\texttt{Proof} =$

...

$\square$

$\texttt{FractionsAbeleanGroupByAddition} :: \forall Z : \texttt{IntegralDomain} . (\mathrm{Frac}(Z), +) : \texttt{Abelean}$

$\texttt{Proof} =$

...

$\square$

$\texttt{FracMultAssoc} :: \forall Z : \texttt{IntegralDomain} . \texttt{fracMult} : \texttt{Associative}\Big(\mathrm{Frac}(Z)\Big)$

$\texttt{Proof} =$

...

$\square$

$\texttt{FracMultCommutes} :: \forall Z : \texttt{IntegralDomain} . \texttt{fracMult} : \texttt{Commutative}\Big(\mathrm{Frac}(Z)\Big)$

$\texttt{Proof} =$

...

$\square$

$\texttt{FracMultDistributesOverFracAdd} :: \forall Z : \texttt{IntegralDomain} . \texttt{fracMult} : \texttt{Distributive}\Big(\mathrm{Frac}(Z), +\Big)$

$\texttt{Proof} =$

$\texttt{Assume}\ \frac{a}{b}, \frac{c}{d}, \frac{f}{g} : \mathrm{Frac}(Z),$

$(*) := \eth\texttt{fracAdd}\eth\texttt{fracMult}\eth\,\mathrm{Frac}(Z)\eth^{-1}\texttt{fracAdd}\eth^{-1}\texttt{fracMult} :$

$$: \frac{a}{b}\left(\frac{c}{d} + \frac{f}{g}\right) = \frac{a}{b}\frac{cg + fd}{dg} = \frac{acg + afd}{dbg} = \frac{bacg + bafd}{db^2g} = \frac{ac}{db} + \frac{af}{bg} = \frac{a}{c}\frac{d}{b} + \frac{a}{b}\frac{f}{g};$$

$\square$

$\texttt{FracMultNeutral} :: \forall Z : \texttt{IntegralDomain} . \frac{1}{1} : \texttt{Neutral}\Big(\mathrm{Frac}(Z), \cdot\Big)$

$\texttt{Proof} =$

...

$\square$

$\texttt{FracIsAField} :: \forall Z : \texttt{IntegralDomain} . \Big(\mathrm{Frac}(Z), +, \cdot\Big) : \texttt{Field}$

$\texttt{Proof} =$

...

$\square$

$\texttt{rationalNumbers} :: \texttt{Field}$

$\texttt{rationalNumbers}\,() = \mathbb{Q} := \mathrm{Frac}\,\mathbb{Z}$

3.2 Order And Topological Structure

$\texttt{CanonicalFractionRepresentation} :: \forall \frac{a}{b} \in \mathbb{Q} \,.\, \exists c \in \mathbb{Z} : \exists n \in \mathbb{N} : \frac{a}{b} = \frac{c}{n}$

$\texttt{Proof} \ =$

$(1) := \eth\mathbb{Q}\left(\frac{a}{b}\right) : b \neq 0,$

$(s, n, 2) := \texttt{IntegerRepresentation}(b) : \sum s \in \mathbb{S}^0 \,.\, \sum n \in \mathbb{Z}_+ \,.\, b = sn,$

$(3) := \texttt{NatIsPositive}(1, 2) : n \in \mathbb{N},$

$(*) := (2)\eth\mathbb{Q}\eth\mathbb{S}^0(s) : \frac{a}{b} = \frac{a}{sn} = \frac{sa}{s^2 n} = \frac{sa}{n};$

$\square$

$\texttt{GreaterRat} :: ?(\mathbb{Q} \times \mathbb{Q})$

$\frac{a}{n}, \frac{b}{m} : \texttt{GreaterRat} \iff \frac{a}{n} \geq \frac{b}{m} \iff am \geq bn$

$\quad \texttt{where}$

$\quad n, m \in \mathbb{N}$

$\texttt{Assume}\ k, l : \mathbb{N},$

$(1) := \texttt{PositiveMult}(k, l) : kl > 0,$

$\texttt{Assume}\ (2) : \frac{a}{n} \geq \frac{b}{m},$

$(3) := \eth\texttt{GreaterRat}(2) : am \geq bn,$

$(4) := \eth\texttt{Field}(\mathbb{Q})\texttt{MultIneq}(1)(3)\eth\texttt{Field} : kalm = klam \geq klbn = lbkn,$

$() := \eth^{-1}\texttt{GreaterRat}(4) : \frac{ka}{kn} \geq \frac{lb}{lm};$

$\rightsquigarrow (2) := I(\Rightarrow) : \frac{a}{n} \geq \frac{b}{m} \Rightarrow \frac{ka}{kn} \geq \frac{lb}{lm},$

$\texttt{Assume}\ (3) : \frac{ka}{kn} \geq \frac{lb}{lm},$

$(4) := \eth\texttt{Field}(\mathbb{Q})\eth\texttt{GreaterRat}(3)\eth\texttt{Field}(\mathbb{Q}) : klam = kalm \geq lbkn = klbn,$

$(5) := \texttt{MultIneq}(1)(4) : am \geq bn,$

$() := \eth^{-1}\texttt{GreaterRat}(5) : \frac{a}{n} \geq \frac{b}{n};$

$\rightsquigarrow (3) := I(\forall)I(\iff)I(\Leftarrow) : \forall l, k \in \mathbb{N} \,.\, \frac{a}{n} \leq \frac{b}{m} \iff \frac{ak}{nk} \leq \frac{bl}{ml};$

$\square$

$\texttt{GreaterRatIsAntisymmetric} :: \texttt{GreaterRat} : \texttt{Antisymmetric}(\mathbb{Q})$

$\texttt{Proof} \ =$

$\texttt{Assume}\ \frac{a}{n}, \frac{b}{m} : \mathbb{Q},$

$\texttt{Assume}\ (1) : \frac{a}{n} \geq \frac{b}{m},$

$\texttt{Assume}\ (2) : \frac{b}{n} \geq \frac{a}{n},$

$(3) := \eth\texttt{GreaterRat}(1) : am \geq bn,$

$(4) := \eth\texttt{GreaterRat}(2) : bn \geq am,$

$(5) := \eth\texttt{Antisymmetric}(\mathbb{Z})(3,4) : am = bn,$

$(6) := \eth\mathbb{Q}(4) : \frac{a}{n} = \frac{b}{m};$

$\square$

$\texttt{GreaterRatIsTransitive} :: \texttt{GreaterRat} : \texttt{Transitive}(\mathbb{Q})$

$\texttt{Proof} \ =$

$\texttt{Assume}\ \frac{a}{n}, \frac{b}{m}, \frac{c}{k} : \mathbb{Q},$

$\texttt{Assume}\ (1) : \frac{a}{n} \geq \frac{b}{m},$

$\texttt{Assume}\ (2) : \frac{b}{m} \geq \frac{c}{k},$

$(3) := \eth\texttt{GreaterRat}(1) : am \geq bn,$

$(4) := \eth\texttt{GreaterRat}(2) : bk \geq cm,$

$(5) := k(3) : amk \geq bnk,$

$(6) := n(4) : bnk \geq cmn,$

$(7) := (5)(6) : amk \geq cmn,$

$(8) := \texttt{MultIneq}(7)(k) : ak \geq cn,$

$(*) := \eth^{-1}\texttt{MultIneq} : \frac{a}{n} \geq \frac{c}{k};$

$\square$

$\texttt{GreaterRatIsOrder} :: \texttt{GreaterRat} : \texttt{Order}(\mathbb{Q})$

$\texttt{Proof} \ =$

$\dots$

$\square$

$\texttt{GreaterRatIsTotal} :: \texttt{GreaterRat} : \texttt{Total}(\mathbb{Q})$

$\texttt{Proof} \ =$

$\dots$

$\square$

$\texttt{orderedRationalNumbers} :: \texttt{OrderedSet}$

$\texttt{orderedRationNumbers}\,() = \mathbb{Q} := (\mathbb{Q}, \texttt{GreaterRat})$

$\texttt{topologicalRationalNumbers} :: \texttt{OrderedSet}$

$\texttt{topologicalRationalNumbers}\,() = \mathbb{Q} := (\mathbb{Q}, \texttt{order}(\mathbb{Q}))$

3.3 Cardinality

$\texttt{CardinalityOfRats} :: |\mathbb{Q}| = \aleph_0$

$\texttt{Proof} \ =$

$(1) := \texttt{CardinalityOfInt} : |\mathbb{Z}| = \aleph_0,$

$f := \texttt{Functor}\,(fraction, ()\,\mathbb{Z}) : \mathbb{Z} \times \mathbb{Z}^{\times} \to \mathbb{Q},$

$g := \Lambda n \in \mathbb{Z} \,.\, \dfrac{n}{1} : \mathbb{Z} \to \mathbb{Q},$

$(2) := \eth\mathbb{Q}\eth f : [f : \mathbb{Z} \times \mathbb{Z}^{\times} \twoheadrightarrow \mathbb{Q},$

$(3) := \eth\mathbb{Q}\eth g : [g : \mathbb{Z} \hookrightarrow \mathbb{Q}],$

$(4) := \texttt{InfCardProduct} : |\mathbb{Z} \times \mathbb{Z}^{\times}| = \aleph_0,$

$(5) := \texttt{SurjCard}(2)(4Z) : |\mathbb{Q}| \leq \aleph_0,$

$(6) := \texttt{InjCard}(3) : |\mathbb{Q}| \geq \aleph_0,$

$(*) := \texttt{CardDoubleIneq}(5)(6) : |\mathbb{Q}| = \aleph_0;$

$\square$

$\texttt{OpenRatsSubsetIsInfinite} :: \forall U : \texttt{Open}(\mathbb{Q}) \,.\, \forall (0) : U \neq \emptyset \,.\, |U| = \aleph_0$

$\texttt{Proof} \ =$

$\ldots$

$\square$

3.4 Additional Algebraic Properties

$\texttt{ratsPower} :: \mathbb{N} \times \mathbb{Q} \to \mathbb{Q}$

$\texttt{ratsPower}\left(n, \frac{a}{b}\right) = \left(\frac{a}{b}\right)^n := \frac{a^n}{b^n}$

$\texttt{ratsPower2} :: \mathbb{Z} \times \mathbb{Q}^{\times} \to \mathbb{Q}^{\times}$

$\texttt{ratsPower2}\left([n,m], \frac{a}{b}\right) = \left(\frac{a}{b}\right)^{[n,m]} := \frac{a^n b^m}{a^m b^n}$

$\texttt{Assume}\ k : \mathbb{Z}_+,$

$(*) := \eth\texttt{ratsPower2}\texttt{Exponentiation}^4(a,n,k)(a,m,k)(b,n,k)(b,m,k)\eth\mathbb{Q}\eth^{-1}\texttt{ratsPower2} :$

$: \left(\frac{a}{b}\right)^{[n+k,m+k]} = \frac{a^{n+k}b^{m+k}}{a^{m+k}b^{n+k}} = \frac{a^n b^m a^k b^k}{a^m b^n a^k b^k} = \frac{a^n b^m}{a^m b^n} = \left(\frac{a}{b}\right)^{[n,m]};$

$\texttt{Exponentiation} :: \forall n,m \in \mathbb{Z} \,.\, \forall \frac{a}{b} \in \mathbb{Q} \,.\, \left(\frac{a}{b}\right)^{n+m} = \left(\frac{a}{b}\right)^n \left(\frac{a}{b}\right)^m$

$\texttt{Proof} \ =$

...

$\square$