```
rect_enumer  THM

⊢  ∀n,m:ℕ+. ∃f:(ℕn×ℕm→ℕ(n·m)). Bij(ℕn×ℕm; ℕ(n·m); f)  by UnivCD
|
1. n : ℕ+
2. m : ℕ+
⊢  ∃f:(ℕn×ℕm→ℕ(n·m)). Bij(ℕn×ℕm; ℕ(n·m); f)
| by Witness λz.1of(z)·m+2of(z)
|
|\
| 3. z : ℕn×ℕm
| ⊢  0≤1of(z)·m+2of(z)  by Analyze 3
| |
| 3. z1 : ℕn
| 4. z2 : ℕm
| ⊢  0≤1of(<z1,z2>)·m+2of(<z1,z2>)  by Analyze 3
| |
| 3. z1 : ℤ
| 4. 0 ≤ z1 < n
| 5. z2 : ℕm
| ⊢   by Analyze 5
| |
| 5. z2 : ℤ
| 6. 0 ≤ z2 < m
| ⊢   by Reduce 0
| |
| ⊢  0≤z1·m+z2  by Analyze 2
| |
| 2. m : ℤ
| 3. 0<m
| 4. z1 : ℤ
| 5. 0 ≤ z1 < n
| 6. z2 : ℤ
| 7. 0 ≤ z2 < m
| ⊢
| | by Inst Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b    {mul_preserves_le}
| |    [0;m;z1]
| |
| 8. z1·0≤z1·m
| ⊢
| | by Inst
| |    Thm* ∀i1,i2,j1,j2:ℤ. i1≤j1 ⇒ i2≤j2 ⇒ i1+i2≤j1+j2
| |    {add_functionality_wrt_le}
| |    [z1·0;0;z1·m;z2]
| |
| 9. z1·0+0≤z1·m+z2
| ⊢   by RWH (RevLemmaC Thm* ∀i:ℤ. i = i+0    {add_ident}) 9
| |
| 9. z1·0≤z1·m+z2
| ⊢   by RWH (RevLemmaC Thm* ∀i:ℤ. 0 = i·0    {zero_ann}) 9
|
|\
| 3. z : ℕn×ℕm
| ⊢  1of(z)·m+2of(z)<n·m  by Analyze 3 THEN Reduce 0
| |
```

```
| 3. z1 : ℕn
| 4. z2 : ℕm
| ⊢  z1·m+z2<n·m  by Analyze 3 THEN Analyze 5
| |
| 3. z1 : ℤ
| 4. 0 ≤ z1 < n
| 5. z2 : ℤ
| 6. 0 ≤ z2 < m
| ⊢   by Inst Thm* ∀i,j:ℤ. i≤j ⟺ i<j+1    {le_to_lt} [z1;n-1]
| |
| 7. z1≤n-1 ⟺ z1<n-1+1
| ⊢   by Analyze 7
| |
| 7. z1≤n-1 ⇒ z1<n-1+1
| 8. (z1≤n-1) ⇐ (z1<n-1+1)
| ⊢   by Analyze 8
| |
| 8. z1≤n-1
| ⊢
| | by Inst Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b    {mul_preserves_le}
| |    [z1;n-1;m]
| |
| 9. m·z1≤m·(n-1)
| ⊢
| | by Inst
| |    Thm* ∀i1,i2,j1,j2:ℤ. i1<j1 ⇒ i2≤j2 ⇒ i1+i2<j1+j2
| |    {add_functionality_wrt_lt}
| |    [z2;m·z1;m;m·(n-1)]
| |
| 10. z2+m·z1<m+m·(n-1)
| ⊢   by Auto
|
.\
. ⊢  Bij(ℕn×ℕm; ℕ(n·m); λz.1of(z)·m+2of(z))  by Unfold ‘biject‘ 0
. |
. ⊢  Inj(ℕn×ℕm; ℕ(n·m); λz.1of(z)·m+2of(z))
. |  & Surj(ℕn×ℕm; ℕ(n·m); λz.1of(z)·m+2of(z))  by Analyze 0
. |
. |\
. | ⊢  Inj(ℕn×ℕm; ℕ(n·m); λz.1of(z)·m+2of(z))  by Unfold ‘inject‘ 0
. | |
. | ⊢  ∀a1,a2:(ℕn×ℕm).
. | |  (λz.1of(z)·m+2of(z))(a1) = (λz.1of(z)·m+2of(z))(a2) ⇒ a1 = a2
. | | by Reduce 0 THEN Analyze 0 THEN Analyze 0
. | |
. | 3. a1 : ℕn×ℕm
. | 4. a2 : ℕn×ℕm
. | ⊢  1of(a1)·m+2of(a1) = 1of(a2)·m+2of(a2) ⇒ a1 = a2  by Analyze 3
. | |
. | 3. a3 : ℕn
. | 4. a4 : ℕm
. | 5. a2 : ℕn×ℕm
. | ⊢  1of(<a3,a4>)·m+2of(<a3,a4>) = 1of(a2)·m+2of(a2) ⇒ <a3,a4> = a2
. | | by Analyze 3
. | |
```

```
. | 3. a3 : ℤ
. | 4. 0 ≤ a3 < n
. | 5. a4 : ℕm
. | 6. a2 : ℕn×ℕm
. | ⊢  by Analyze 5
. | |
. | 5. a4 : ℤ
. | 6. 0 ≤ a4 < m
. | 7. a2 : ℕn×ℕm
. | ⊢  by Analyze 7
. | |
. | 7. a5 : ℕn
. | 8. a6 : ℕm
. | ⊢  1of(<a3,a4>)·m+2of(<a3,a4>) = 1of(<a5,a6>)·m+2of(<a5,a6>) ⇒
. | |  <a3,a4> = <a5,a6>  by Analyze 7
. | |
. | 7. a5 : ℤ
. | 8. 0 ≤ a5 < n
. | 9. a6 : ℕm
. | ⊢  by Analyze 9
. | |
. | 9. a6 : ℤ
. | 10. 0 ≤ a6 < m
. | ⊢  by Reduce 0
. | |
. | ⊢  a3·m+a4 = a5·m+a6 ⇒ <a3,a4> = <a5,a6>  by Analyze 0
. | |
. | |\
. | | 11. a3·m+a4 = a5·m+a6
. | | ⊢  <a3,a4> = <a5,a6>  by Analyze
. | | |
. | | |\
. | | | ⊢  a3 = a5
. | | | | by Inst
. | | | |    Thm* ∀a:ℕ, n:ℕ⁺, p,q:ℕ. Div(a;n;p) ⇒ Div(a;n;q) ⇒ p = q
. | | | |    {div_unique}
. | | | |    [a3·m+a4;m;a3;a5]
. | | | |
. | | | |\
. | | | | .....antecedent .....
. | | | | ⊢  Div(a3·m+a4;m;a3)  by Unfold ‘div_nrel‘ 0
. | | | |
. | | | .\
. | | | . .....antecedent .....
. | | | . ⊢  Div(a3·m+a4;m;a5)  by Unfold ‘div_nrel‘ 0
. | | |
. | | .\
. | | . ⊢  a4 = a6
. | | . | by Inst
. | | . |    Thm* ∀a:ℤ, b:ℤ⁻⁰. |a|<|b| ⇒ (a rem b) = a
. | | . |    {rem_base_case_z}
. | | . |    [a4;m]
. | | . |
. | | . |\
. | | . | 4. 0≤a3
```

```
. | | . | 5. a3<n
. | | . | 6. a4 : ℤ
. | | . | 7. 0≤a4
. | | . | 8. a4<m
. | | . | 9. a5 : ℤ
. | | . | 10. 0≤a5
. | | . | 11. a5<n
. | | . | 12. a6 : ℤ
. | | . | 13. 0≤a6
. | | . | 14. a6<m
. | | . | 15. a3·m+a4 = a5·m+a6
. | | . | ⊢  |a4|<|m|  by Unfold ‘absval‘ 0
. | | . | |
. | | . | ⊢  if 0≤z a4→ a4 else -a4 fi<if 0≤z m→ m else -m fi
. | | . |   by SplitOnConclITE THEN SplitOnConclITE
. | | . |
. | | . .\
. | | . . 12. (a4 rem m) = a4
. | | . . ⊢
. | | . . | by Inst
. | | . . |    Thm* ∀a:ℤ, n:ℤ-0. |a|<|n| ⇒ (a rem n) = a
. | | . . |    {rem_gen_base_case}
. | | . . |    [a6;m]
. | | . . |
. | | . . |\
. | | . . | 4. 0≤a3
. | | . . | 5. a3<n
. | | . . | 6. a4 : ℤ
. | | . . | 7. 0≤a4
. | | . . | 8. a4<m
. | | . . | 9. a5 : ℤ
. | | . . | 10. 0≤a5
. | | . . | 11. a5<n
. | | . . | 12. a6 : ℤ
. | | . . | 13. 0≤a6
. | | . . | 14. a6<m
. | | . . | 15. a3·m+a4 = a5·m+a6
. | | . . | 16. (a4 rem m) = a4
. | | . . | ⊢  |a6|<|m|  by Unfold ‘absval‘ 0
. | | . . | |
. | | . . | ⊢  if 0≤z a6→ a6 else -a6 fi<if 0≤z m→ m else -m fi
. | | . . |   by SplitOnConclITE THEN SplitOnConclITE
. | | . . |
. | | . . .\
. | | . . . 13. (a6 rem m) = a6
. | | . . . ⊢   by Analyze
. | | . . . |
. | | . . . |\
. | | . . . | ⊢  a4 = a6  by RWH (RevHypC 12) 0
. | | . . . | |
. | | . . . | ⊢  (a4 rem m) = a6  by RWH (RevHypC 13) 0
. | | . . . | |
. | | . . . | ⊢  (a4 rem m) = (a6 rem m)
. | | . . . | | by Inst
. | | . . . | |    Thm* ∀a,b:ℕ, n:ℕ+. ((a+b·n) rem n) = (a rem n)
```

```
. | | . . . | |    {rem_invariant}
. | | . . . | |    [a4;a3;m]
. | | . . . | |
. | | . . . | 14. ((a4+a3·m) rem m) = (a4 rem m)
. | | . . . | ⊢   by RWH (RevHypC 14) 0
. | | . . . | |
. | | . . . | ⊢  ((a4+a3·m) rem m) = (a6 rem m)
. | | . . . | | by Assert (a4+a3·m = a3·m+a4)
. | | . . . | |
. | | . . . | |\
. | | . . . | | .....assertion .....
. | | . . . | | ⊢  a4+a3·m = a3·m+a4  by Auto
. | | . . . | |
. | | . . . | .\
. | | . . . | . 15. a4+a3·m = a3·m+a4
. | | . . . | . ⊢   by RWH (HypC 15) 0
. | | . . . | . |
. | | . . . | . ⊢  ((a3·m+a4) rem m) = (a6 rem m)  by RWH (HypC 11) 0
. | | . . . | . |
. | | . . . | . ⊢  ((a5·m+a6) rem m) = (a6 rem m)
. | | . . . | . | by Assert (a5·m+a6 = a6+a5·m)
. | | . . . | . |
. | | . . . | . |\
. | | . . . | . | .....assertion .....
. | | . . . | . | ⊢  a5·m+a6 = a6+a5·m  by Auto
. | | . . . | . |
. | | . . . | . .\
. | | . . . | . . 16. a5·m+a6 = a6+a5·m
. | | . . . | . . ⊢   by RWH (HypC 16) 0
. | | . . . | . . |
. | | . . . | . . ⊢  ((a6+a5·m) rem m) = (a6 rem m)
. | | . . . | . .   by RWH
. | | . . . | . .      (LemmaC
. | | . . . | . .       Thm* ∀a,b:ℕ, n:ℕ+. ((a+b·n) rem n) = (a rem n)
. | | . . . | . .       {rem_invariant})
. | | . . . | . .      0
. | | . . . |
. | | . . . .\
. | | . . . . .....set predicate .....
. | | . . . . ⊢  0 ≤ a4 < m  by Auto
. | |
. | |\
. | | 4. 0≤a3
. | | 5. a3<n
. | | 6. a4 : ℤ
. | | 7. 0≤a4
. | | 8. a4<m
. | | 9. a5 : ℤ
. | | 10. 0≤a5
. | | 11. a5<n
. | | 12. a6 : ℤ
. | | 13. 0≤a6
. | | 14. a6<m
. | | ⊢  0≤a3·m+a4  by Analyze 2
. | | |
```

```
. | | 2. m : ℤ
. | | 3. 0<m
. | | 4. a3 : ℤ
. | | 5. 0≤a3
. | | 6. a3<n
. | | 7. a4 : ℤ
. | | 8. 0≤a4
. | | 9. a4<m
. | | 10. a5 : ℤ
. | | 11. 0≤a5
. | | 12. a5<n
. | | 13. a6 : ℤ
. | | 14. 0≤a6
. | | 15. a6<m
. | | ⊢   by Inst Thm* ∀a,b:ℕ. 0≤a·b    {mul_bounds_1a} [a3;m]
. | | |
. | | 16. 0≤a3·m
. | | ⊢   by Auto
. | |
. | |\
. | | 4. 0≤a3
. | | 5. a3<n
. | | 6. a4 : ℤ
. | | 7. 0≤a4
. | | 8. a4<m
. | | 9. a5 : ℤ
. | | 10. 0≤a5
. | | 11. a5<n
. | | 12. a6 : ℤ
. | | 13. 0≤a6
. | | 14. a6<m
. | | ⊢  a3·m+a4<n·m
. | | | by Inst Thm* ∀i,j:ℤ. i≤j ⟺ i<j+1    {le_to_lt} [a3;n-1]
. | | |
. | | 15. a3≤n-1 ⟺ a3<n-1+1
. | | ⊢   by Analyze 15
. | | |
. | | 15. a3≤n-1 ⇒ a3<n-1+1
. | | 16. (a3≤n-1) ⇐ (a3<n-1+1)
. | | ⊢   by Analyze 16
. | | |
. | | 16. a3≤n-1
. | | ⊢
. | | | by Inst Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b    {mul_preserves_le}
. | | |    [a3;n-1;m]
. | | |
. | | 17. m·a3≤m·(n-1)
. | | ⊢   by Auto
. | |
. | |\
. | | 4. 0≤a3
. | | 5. a3<n
. | | 6. a4 : ℤ
. | | 7. 0≤a4
. | | 8. a4<m
```

```
. | | 9. a5 : ℤ
. | | 10. 0≤a5
. | | 11. a5<n
. | | 12. a6 : ℤ
. | | 13. 0≤a6
. | | 14. a6<m
. | | ⊢  0≤a5·m+a6
. | |   by Inst Thm* ∀a,b:ℕ. 0≤a·b    {mul_bounds_1a} [a5;m]
. | |
. | .\
. | . 4. 0≤a3
. | . 5. a3<n
. | . 6. a4 : ℤ
. | . 7. 0≤a4
. | . 8. a4<m
. | . 9. a5 : ℤ
. | . 10. 0≤a5
. | . 11. a5<n
. | . 12. a6 : ℤ
. | . 13. 0≤a6
. | . 14. a6<m
. | . ⊢  a5·m+a6<n·m
. | . | by Inst Thm* ∀i,j:ℤ. i≤j ⟺ i<j+1    {le_to_lt} [a5;n-1]
. | . |
. | . 15. a5≤n-1 ⟺ a5<n-1+1
. | . ⊢   by Analyze 15
. | . |
. | . 15. a5≤n-1 ⇒ a5<n-1+1
. | . 16. (a5≤n-1) ⇐ (a5<n-1+1)
. | . ⊢   by Analyze 16
. | . |
. | . 16. a5≤n-1
. | . ⊢
. | .   by Inst Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b    {mul_preserves_le}
. | .      [a5;n-1;m]
. |
. .\
. . ⊢  Surj(ℕn×ℕm; ℕ(n·m); λz.1of(z)·m+2of(z))  by Unfold ‘surject‘ 0
. . |
. . ⊢  ∀b:ℕ(n·m). ∃a:(ℕn×ℕm). (λz.1of(z)·m+2of(z))(a) = b
. . | by Analyze 0
. . |
. . 3. b : ℕ(n·m)
. . ⊢  ∃a:(ℕn×ℕm). (λz.1of(z)·m+2of(z))(a) = b  by Reduce 0
. . |
. . ⊢  ∃a:(ℕn×ℕm). 1of(a)·m+2of(a) = b  by Witness <b ÷ m,b rem m>
. . |
. . |\
. . | ⊢  0≤(b ÷ m)
. . |   by Inst Thm* ∀a:ℕ, n:ℕ+. 0≤(a ÷ n)    {div_bounds_1} [b;m]
. . |
. . |\
. . | ⊢  (b ÷ m)<n  by Analyze 3
. . | |
. . | 3. b : ℤ
```

```
. . | 4. 0 ≤ b < n·m
. . | ⊢
. . | | by Inst
. . | |    Thm* ∀a:ℤ, n:ℤ-0. a = (a ÷ n)·n+(a rem n)    {div_rem_sum}
. . | |    [b;m]
. . | |
. . | 5. b = (b ÷ m)·m+(b rem m)
. . | ⊢   by Analyze 4
. . | |
. . | 4. 0≤b
. . | 5. b<n·m
. . | 6. b = (b ÷ m)·m+(b rem m)
. . | ⊢   by RWH (HypC 6) 5
. . | |
. . | 5. (b ÷ m)·m+(b rem m)<n·m
. . | 6. b = (b ÷ m)·m+(b rem m)
. . | ⊢

. . | | by Inst
. . | |    Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . | |    {rem_bounds_1}
. . | |    [b;m]
. . | |
. . | 7. 0≤(b rem m) & (b rem m)<m
. . | ⊢   by Analyze 7
. . | |
. . | 7. 0≤(b rem m)
. . | 8. (b rem m)<m
. . | ⊢
. . | | by Inst Thm* ∀i,j:ℤ. i≥j ⟺ -i≤-j    {minus_mono_wrt_le}
. . | |    [b rem m;0]
. . | |
. . | 9. (b rem m)≥0 ⟺ -(b rem m)≤-0
. . | ⊢   by Analyze 9
. . | |
. . | 9. (b rem m)≥0 ⇒ -(b rem m)≤-0
. . | 10. ((b rem m)≥0) ⇐ (-(b rem m)≤-0)
. . | ⊢   by Analyze 9
. . | |
. . | 9. ((b rem m)≥0) ⇐ (-(b rem m)≤-0)
. . | 10. -(b rem m)≤-0
. . | ⊢
. . | | by Inst
. . | |    Thm* ∀i1,i2,j1,j2:ℤ. i1<j1 ⇒ i2≤j2 ⇒ i1+i2<j1+j2
. . | |    {add_functionality_wrt_lt}
. . | |    [(b ÷ m)·m+(b rem m);-(b rem m);n·m;0]
. . | |
. . | 11. (b ÷ m)·m+(b rem m)+-(b rem m)<n·m+0
. . | ⊢   by Assert ((b ÷ m)·m<n·m)
. . | |
. . | |\
. . | | .....assertion .....
. . | | ⊢  (b ÷ m)·m<n·m  by Auto
. . | |
. . | .\
. . | . 12. (b ÷ m)·m<n·m
```

```
. . | . ⊢
. . | .   by Inst
. . | .      Thm* ∀a,b:ℤ, n:ℕ+. n·a<n·b ⇒ a<b    {mul_cancel_in_lt}
. . | .      [b ÷ m;n;m]
. . |
. . |\
. . | ⊢  0≤(b rem m)
. . | | by Inst
. . | |    Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . | |    {rem_bounds_1}
. . | |    [b;m]
. . | |
. . | 4. 0≤(b rem m) & (b rem m)<m
. . | ⊢   by Analyze 4
. . |
. . |\
. . | ⊢  (b rem m)<m
. . |   by Inst
. . |      Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . |      {rem_bounds_1}
. . |      [b;m]
. . |
. . |\
. . | ⊢  1of(<b ÷ m,b rem m>)·m+2of(<b ÷ m,b rem m>) = b  by Reduce 0
. . | |
. . | ⊢  (b ÷ m)·m+(b rem m) = b
. . |   by Inst
. . |      Thm* ∀a:ℤ, n:ℤ-0. a = (a ÷ n)·n+(a rem n)    {div_rem_sum}
. . |      [b;m]
. . |
. . |\
. . | 4. a : ℕn×ℕm
. . | ⊢  0≤1of(a)·m+2of(a)  by Analyze 4 THEN Reduce 0
. . | |
. . | 4. a1 : ℕn
. . | 5. a2 : ℕm
. . | ⊢  0≤a1·m+a2
. . |   by Inst Thm* ∀a,b:ℕ. 0≤a·b    {mul_bounds_1a} [a1;m]
. . |
. . . \
. . . 4. a : ℕn×ℕm
. . . ⊢  1of(a)·m+2of(a)<n·m  by Analyze 4 THEN Reduce 0
. . . |
. . . 4. a1 : ℕn
. . . 5. a2 : ℕm
. . . ⊢  a1·m+a2<n·m  by Analyze 4
. . . |
. . . 4. a1 : ℤ
. . . 5. 0 ≤ a1 < n
. . . 6. a2 : ℕm
. . . ⊢   by Analyze 6
. . . |
. . . 6. a2 : ℤ
. . . 7. 0 ≤ a2 < m
. . . ⊢
```

```
. . . | by Inst Thm* ∀i,j:ℤ. i≤j ⟺ i<j+1    {le_to_lt} [a1;n-1]
. . . |    THEN
. . . |    Analyze 8
. . . |
. . . 8. a1≤n-1 ⇒ a1<n-1+1
. . . 9. (a1≤n-1) ⇐ (a1<n-1+1)
. . . ⊢   by Analyze 9

. . . |
. . . 9. a1≤n-1
. . . ⊢
. . . | by Inst Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b    {mul_preserves_le}
. . . |    [a1;n-1;m]
. . . |
. . . 10. m·a1≤m·(n-1)
. . . ⊢
. . . | by Inst
. . . |    Thm* ∀i1,i2,j1,j2:ℤ. i1<j1 ⇒ i2≤j2 ⇒ i1+i2<j1+j2
. . . |    {add_functionality_wrt_lt}
. . . |    [a2;a1·m;m;m·(n-1)]
. . . |
. . . 11. a2+a1·m<m+m·(n-1)
. . . ⊢   by Auto
END
```