CHAPTER 1

DIVISION

This chapter introduces and develops division. Notable propositions include:
P10: Reflexivity of Division
P23: Antisymmetry of Division
P24: Transitivity of Division
P29: Division of Additive Linear Combinations
P30: Division of Subtracting Linear Combinations
P51-P55: Division and 0 Remainders
P57: Lemma for establishing Euclid's theorem that the prime numbers are infinite

1. | represents division.

$ | ; **n**|**m** ; ∃x (**n** x x) = **m**

2.

⊢ ∀n∀m (n|m ⇒ ω[n] & ω[m])

n,**m**	,! 1 (Prem)
n|**m**	,! 2 (Prem)
∃x (**n** x x) = **m**	,! 3 ($E: P1,2)
(**n** x **x**) = **m**	,! 4 (∃E: 3)
ω[**n**] & ω[**x**]	,! 5 (𝕋E: V7.9,4)
ω[**n**]	,! 6 (&E: 5)
((**n** x **x**) = **m** ⇒ ω[**m**])	,! 7 (∀E: V7.12)
(**n** x **x**) = **m** ⇒ ω[**m**]	,! 8 (()E: 7)
ω[**m**]	,! 9 (⇒E: 4,8)
ω[**n**] & ω[**m**]	,! 10 (&I: 6,9)
n|**m** ⇒ ω[**n**] & ω[**m**]	,! 11 (⇒I: 2,10)
(**n**|**m** ⇒ ω[**n**] & ω[**m**])	,! 12 (()I: 11)
∀n∀m (n|m ⇒ ω[n] & ω[m])	! 13 (∀I: 1,12)

□

3.

⊢ ∀n∀m (n|m ⇒ ω[n])

n,**m**	,! 1 (Prem)
n|**m**	,! 2 (Prem)

(**n**|**m** ⇒ ω[**n**] & ω[**m**]) ,! 3 (∀E: P2) ¡

n|**m** ⇒ ω[**n**] & ω[**m**] ,! 4 (()E: 3) ¡

ω[**n**] & ω[**m**] ,! 5 (⇒E: 2,4) ¡

ω[**n**] ,! 6 (&E: 5) ¡

n|**m** ⇒ ω[**n**] ,! 7 (⇒I: 2,6) ¡

(**n**|**m** ⇒ ω[**n**]) ,! 8 (()I: 7) ¡

∀n∀m (n|m ⇒ ω[n]) ! 9 (∀I: 1,8) ¡

□

! **4.** ¡

⊢ ∀n∀m (n|m ⇒ ω[m]) ¡

n,**m** ,! 1 (Prem) ¡

n|**m** ,! 2 (Prem) ¡

(**n**|**m** ⇒ ω[**n**] & ω[**m**]) ,! 3 (∀E: P2) ¡

n|**m** ⇒ ω[**n**] & ω[**m**] ,! 4 (()E: 3) ¡

ω[**n**] & ω[**m**] ,! 5 (⇒E: 2,4) ¡

ω[**m**] ,! 6 (&E: 5) ¡

n|**m** ⇒ ω[**m**] ,! 7 (⇒I: 2,6) ¡

(**n**|**m** ⇒ ω[**m**]) ,! 8 (()I: 7) ¡

∀n∀m (n|m ⇒ ω[m]) ! 9 (∀I: 1,8) ¡

□

! The $E and $I rules, applied to the definition of division (P1), justify passage from **n**|**m** to ∃x (**n** x x) = **m** and vice versa. Propositions P5 through P7 are useful when the **n** is on the right-hand rather than the left-hand side of the product. ¡

! **5.** ¡

⊢ ∀n∀m (n|m ⇒ ∃x (x x n) = m) ¡

n,**m** ,! 1 (Prem) ¡

n|**m** ,! 2 (Prem) ¡

∃x (**n** x x) = **m** ,! 3 ($E: P1,2) ¡

(**n** x **x**) = **m** ,! 4 (∃E: 3) ¡

((**n** x **x**) = **m** ⇒ (**x** x **n**) = **m**) ,! 5 (∀E: V8.26) ¡

(**n** x **x**) = **m** ⇒ (**x** x **n**) = **m** ,! 6 (()E: 5) ¡

(**x** x **n**) = **m** ,! 7 (⇒E: 4,6) ¡

∃x (x x **n**) = **m** ,! 8 (∃I: 7) ¡

n|**m** ⇒ ∃x (x x **n**) = **m** ,! 9 (⇒I: 2,8) ¡

(**n**|**m** ⇒ ∃x (x x **n**) = **m**) ,! 10 (()I: 9) ¡

∀n∀m (n|m ⇒ ∃x (x x n) = m) ! 11 (∀I: 1,10) ¡

□

! **6.** ¡

⊢ ∀n∀m∀x ((x x n) = m ⇒ n|m) ¡

n,**m**,**x** ,! 1 (Prem) ¡

(**x** x **n**) = **m** ,! 2 (Prem) ¡

((**x** x **n**) = **m** ⇒ (**n** x **x**) = **m**) ,! 3 (∀E: V8.26) ¡

(**x** x **n**) = **m** ⇒ (**n** x **x**) = **m** ,! 4 (()E: 3) ¡

(**n** x **x**) = **m** ,! 5 (⇒E: 2,4) ¡

∃x (**n** x x) = **m** ,! 6 (∃I: 5) ¡

n|**m** ,! 7 (S I: P1,7) ¡

(**x** x **n**) = **m** ⇒ **n**|**m** ,! 8 (⇒I: 2,7) ¡

((**x** x **n**) = **m** ⇒ **n**|**m**) ,! 9 (()I: 8) ¡

∀n∀m∀x ((x x n) = m ⇒ n|m) ! 10 (∀I: 1,9) ¡

□

! **7.** ¡

⊢ ∀n∀m∀x (m = (x x n) ⇒ n|m) ¡

n,**m**,**x** ,! 1 (Prem) ¡

m = (**x** x **n**) ,! 2 (Prem) ¡

m = **m** ,! 3 (=I) ¡

(**x** x **n**) = **m** ,! 4 (=E: 2,3) ¡

((**x** x **n**) = **m** ⇒ **n**|**m**) ,! 5 (∀E: P6) ¡

(**x** x **n**) = **m** ⇒ **n**|**m** ,! 6 (()E: 5)

n|**m** ,! 7 (⇒E: 4,6)

m = (**x** x **n**) ⇒ **n**|**m** ,! 8 (⇒I: 2,7)

(**m** = (**x** x **n**) ⇒ **n**|**m**) ,! 9 (()I: 8)

∀n∀m∀x (m = (x x n) ⇒ n|m) ! 10 (∀I: 1,9)

□

! **8.**

⊢ ∀n∀m (ω[n] & ω[m] ⇒ n|(n x m))

n,**m** ,! 1 (Prem)

ω[**n**] & ω[**m**] ,! 2 (Prem)

(**n** x **m**) = (**n** x **m**) ,! 3 (=I; (**n** x **m**): V7.9,2)

∃x (**n** x x) = (**n** x **m**) ,! 4 (∃I: 3)

n|(**n** x **m**) ,! 5 (𝕊I: P1,4)

ω[**n**] & ω[**m**] ⇒ **n**|(**n** x **m**) ,! 6 (⇒I: 2,5)

(ω[**n**] & ω[**m**] ⇒ **n**|(**n** x **m**)) ,! 7 (()I: 6)

∀n∀m (ω[n] & ω[m] ⇒ n|(n x m)) ! 8 (∀I: 1,7)

□

! **9.**

⊢ ∀n∀m (ω[n] & ω[m] ⇒ n|(m x n))

n,**m** ,! 1 (Prem)

ω[**n**] & ω[**m**] ,! 2 (Prem)

(ω[**n**] & ω[**m**] ⇒ **n**|(**n** x **m**)) ,! 3 (∀E: P8)

ω[**n**] & ω[**m**] ⇒ **n**|(**n** x **m**) ,! 4 (()E: 3)

n|(**n** x **m**) ,! 5 (⇒E: 2,4)

(ω[**n**] & ω[**m**] ⇒ ⇒ (**n** x **m**) = (**m** x **n**)) ,! 6 (∀E: V8.25)

ω[**n**] & ω[**m**] ⇒ ⇒ (**n** x **m**) = (**m** x **n**) ,! 7 (()E: 6)

```
    (n x m) = (m x n)                    ,! 8 (⇒E: 2,7)     ¡
    n|(m x n)                            ,! 9 (=E: 5,8)     ¡
  ω[n] & ω[m] ⇒ n|(m x n)                ,! 10 (⇒I: 2,9)    ¡
  ( ω[n] & ω[m] ⇒ n|(m x n) )            ,! 11 (()I: 10)    ¡
∀n∀m ( ω[n] & ω[m] ⇒ n|(m x n) )          ! 12 (∀I: 1,11)   ¡
□
! 10. Reflexivity of Division.                               ¡
⊢ ∀n ( ω[n] ⇒ n|n )                                         ¡
  n                                      ,! 1 (Prem)        ¡
    ω[n]                                 ,! 2 (Prem)        ¡
    ( ω[n] ⇒ (n x 1) = n )               ,! 3 (∀E: V8.18)   ¡
    ω[n] ⇒ (n x 1) = n                   ,! 4 (()E: 3)      ¡
    (n x 1) = n                          ,! 5 (⇒E: 2,4)     ¡
    ∃x (n x x) = n                       ,! 6 (∃I: 5)       ¡
    n|n                                  ,! 7 (§I: P1,6)    ¡
  ω[n] ⇒ n|n                             ,! 8 (⇒I: 2,7)     ¡
  ( ω[n] ⇒ n|n )                         ,! 9 (()I: 8)      ¡
∀n ( ω[n] ⇒ n|n )                        ,! 10 (∀I: 1,9)    ¡
□
! 11. Every finite number divides 0.                         ¡
⊢ ∀n ( ω[n] ⇒ n|0 )                                         ¡
  n                                      ,! 1 (Prem)        ¡
    ω[n]                                 ,! 2 (Prem)        ¡
    ( ω[n] ⇒ (n x 0) = 0 )               ,! 3 (∀E: V8.4)    ¡
    ω[n] ⇒ (n x 0) = 0                   ,! 4 (()E: 3)      ¡
    (n x 0) = 0                          ,! 5 (⇒E: 2,4)     ¡
    ∃x (n x x) = 0                       ,! 6 (∃I: 5)       ¡
    n|0                                  ,! 7 (§I: P1,6)    ¡
```

  ω[**n**] ⇒ **n**|0 ,! 8 (⇒I: 2,7) ¡

  (ω[**n**] ⇒ **n**|0) ,! 9 (()I: 8) ¡

∀n (ω[n] ⇒ n|0) ! 10 (∀I: 1,9) ¡

□

! **12.** The only number divisible by 0 is 0. ¡

⊢ ∀n (0|n ⇒ n = 0) ¡

  n ,! 1 (Prem) ¡

    0|**n** ,! 2 (Prem) ¡

    ∃x (0 x x) = **n** ,! 3 (∃E: P1,2) ¡

    (0 x **x**) = **n** ,! 4 (∃E: 3) ¡

    ω[0] & ω[**x**] ,! 5 (𝕋E: V7.9,4) ¡

    ω[**x**] ,! 6 (&E: 5) ¡

    (ω[**x**] ⇒ (0 x **x**) = 0) ,! 7 (∀E: V8.3) ¡

    ω[**x**] ⇒ (0 x **x**) = 0 ,! 8 (()E: 7) ¡

    (0 x **x**) = 0 ,! 9 (⇒E: 6,8) ¡

    n = 0 ,! 10 (=E: 4,9) ¡

  0|**n** ⇒ **n** = 0 ,! 11 (⇒I: 2,10) ¡

  (0|**n** ⇒ **n** = 0) ,! 12 (()I: 11) ¡

∀n (0|n ⇒ n = 0) ! 13 (∀I: 1,12) ¡

□

! **13.** ¡

⊢ ∀n∀m (n|m & ¬ m = 0 ⇒ ¬ n = 0) ¡

  n,**m** ,! 1 (Prem) ¡

    n|**m** & ¬ **m** = 0 ,! 2 (Prem) ¡

    n|**m** ,! 3 (&E: 2) ¡

    ¬ **m** = 0 ,! 4 (&E: 2) ¡

      n = 0 ,! 5 (Prem) ¡

      0|**m** ,! 6 (=E: 3,5) ¡

      (0|**m** ⇒ **m** = 0) ,! 7 (∀E: P12) ¡

```
      0|m ⇒ m = 0                          ,! 8 (()E: 7)      ¡
      m = 0                                ,! 9 (⇒E: 6,8)     ¡
      ℱ                                    ,! 10 (ℱI: 4,9)    ¡
    n = 0 ⇒ ℱ                              ,! 11 (⇒I: 5,10)   ¡
    ¬ n = 0                                ,! 12 (¬I: 11)     ¡
  n|m & ¬ m = 0 ⇒ ¬ n = 0                   ,! 13 (⇒I: 2,12)   ¡
  ( n|m & ¬ m = 0 ⇒ ¬ n = 0 )               ,! 14 ()I: 13)     ¡
∀n∀m ( n|m & ¬ m = 0 ⇒ ¬ n = 0 )             ! 15 (∀I: 1,14)    ¡
□
! 14. 1 divides every finite number.                             ¡
⊢ ∀n ( ω[n] ⇒ 1|n )                                             ¡
  n                                        ,! 1 (Prem)        ¡
    ω[n]                                   ,! 2 (Prem)        ¡
    ( ω[n] ⇒ (1 x n) = n )                 ,! 3 (∀E: V8.14)   ¡
    ω[n] ⇒ (1 x n) = n                     ,! 4 (()E: 3)      ¡
    (1 x n) = n                            ,! 5 (⇒E: 2,4)     ¡
    ∃x (1 x x) = n                         ,! 6 (∃I: 5)       ¡
    1|n                                    ,! 7 ($I: P1,6)    ¡
  ω[n] ⇒ 1|n                               ,! 8 (⇒I: 2,7)     ¡
  ( ω[n] ⇒ 1|n )                           ,! 9 (()I: 8)      ¡
∀n ( ω[n] ⇒ 1|n )                           ! 10 (∀I: 1,9)     ¡
□
! 15. The only number which divides 1 is 1.                      ¡
⊢ ∀n ( n|1 ⇒ n = 1 )                                            ¡
  n                                        ,! 1 (Prem)        ¡
    n|1                                    ,! 2 (Prem)        ¡
    ∃x (n x x) = 1                         ,! 3 ($E: P1,2)    ¡
    (n x x) = 1                            ,! 4 (∃E: 3)       ¡
```

```
    ( (n x x) = 1 ⇒ n = 1 )              ,! 5 (∀E: V8.63)    ¡
    (n x x) = 1 ⇒ n = 1                  ,! 6 (()E: 5)       ¡
    n = 1                                ,! 7 (⇒E: 4,6)      ¡
  n|1 ⇒ n = 1                            ,! 8 (⇒I: 2,7)      ¡
  ( n|1 ⇒ n = 1 )                        ,! 9 (()I: 8)       ¡
∀n ( n|1 ⇒ n = 1 )                        ! 10 (∀I: 1,9)     ¡
□
! P16 through P21 are divisions with specific numbers.        ¡
! 16.                                                         ¡
⊢ 0|0                                                        ¡
( ω[0] ⇒ 0|0 )                           ,! 1 (∀E: P10)      ¡
ω[0] ⇒ 0|0                               ,! 2 (()E: 1)       ¡
0|0                                      ,! 3 (⇒E: ω0,2)     ¡
□
! 17.                                                        ¡
⊢ 1|0                                                        ¡
( ω[1] ⇒ 1|0 )                           ,! 1 (∀E: P11)      ¡
ω[1] ⇒ 1|0                               ,! 2 (()E: 1)       ¡
1|0                                      ,! 3 (⇒E: IV9.2,2)  ¡
□
! 18.                                                        ¡
⊢ 2|0                                                        ¡
( ω[2] ⇒ 2|0 )                           ,! 1 (∀E: P11)      ¡
ω[2] ⇒ 2|0                               ,! 2 (()E: 1)       ¡
2|0                                      ,! 3 (⇒E: IV9.11,2)
                                                             ¡
□
! 19.                                                        ¡
⊢ 1|1                                                        ¡
```

(ω[1] ⇒ 1|1) ,! 1 (∀E: P10) ¡

ω[1] ⇒ 1|1 ,! 2 (()E: 1) ¡

1|1 ,! 3 (⇒E: IV9.2,2) ¡

□

! **20.** ¡

⊢ 1|2 ¡

(ω[2] ⇒ 1|2) ,! 1 (∀E: P14) ¡

ω[2] ⇒ 1|2 ,! 2 (()E: 1) ¡

1|2 ,! 3 (⇒E: IV9.11,2) ¡

□

! **21.** ¡

⊢ 2|2 ¡

(ω[2] ⇒ 2|2) ,! 1 (∀E: P10) ¡

ω[2] ⇒ 2|2 ,! 2 (()E: 1) ¡

2|2 ,! 3 (⇒E: IV9.11,2) ¡

□

! **22.** P22 does not appeal to any proposition, but it belongs to VI1, since it uses a symbol which is only introduced in this chapter. There is no good position for it, so it is put here. ¡

⊢ ∀n∀m (n|m ∨ ¬ n|m) ¡

n,**m** ,! 1 (Prem) ¡

¬ (**n**|**m** ∨ ¬ **n**|**m**) ,! 2 (Prem) ¡

n|**m** ,! 3 (Prem) ¡

n|**m** ∨ ¬ **n**|**m** ,! 4 (∨I: 3) ¡

(**n**|**m** ∨ ¬ **n**|**m**) ,! 5 ()I: 4) ¡

ℱ ,! 6 (ℱI: 2,5) ¡

n|**m** ⇒ ℱ ,! 7 (⇒I: 6) ¡

¬ **n**|**m** ,! 8 (¬I: 7) ¡

n|**m** ∨ ¬ **n**|**m** ,! 9 (∨I: 8) ¡

(**n**|**m** ∨ ¬ **n**|**m**) ,! 10 (()I: 9) ¡

ℱ ,! 11 (ℱI: 2,10) ¡

¬ (**n**|**m** ∨ ¬ **n**|**m**) ⇒ ℱ ,! 12 (⇒I: 2,11) ¡

¬¬ (**n**|**m** ∨ ¬ **n**|**m**) ,! 13 (¬I: 12) ¡

(**n**|**m** ∨ ¬ **n**|**m**) ,! 14 (¬E: 13) ¡

∀n∀m (n|m ∨ ¬ n|m) ! 15 (∀I: 1,14) ¡

□

! **23. Antisymmetry of Division.** ¡

⊢ ∀n∀m∀k (n|m & m|n ⇒ n = m) ¡

n,**m**,**k** ,! 1 (Prem) ¡

n|**m** & **m**|**n** ,! 2 (Prem) ¡

n|**m** ,! 3 (&E: 2) ¡

m|**n** ,! 4 (&E: 2) ¡

(**n** = 0 ∨ ¬ **n** = 0) ,! 5 (∀E: I3.4) ¡

n = 0 ∨ ¬ **n** = 0 ,! 6 (()E: 5) ¡

n = 0 ,! 7 (Prem) ¡

0|**m** ,! 8 (=E: 3,7) ¡

(0|**m** ⇒ **m** = 0) ,! 9 (∀E: P12) ¡

0|**m** ⇒ **m** = 0 ,! 10 (()E: 9) ¡

m = 0 ,! 11 (⇒E: 8,10) ¡

n = **m** ,! 12 (=E: 7,11) ¡

n = 0 ⇒ **n** = **m** ,! 13 (⇒I: 7,12) ¡

¬ **n** = 0 ,! 14 (Prem) ¡

∃x (**n** x x) = **m** ,! 15 ($E: P1,3) ¡

(**n** x **a**) = **m** ,! 16 (∃E: 15) ¡

∃x (**m** x x) = **n** ,! 17 ($E: P1,4) ¡

(**m** x **b**) = **n** ,! 18 (∃E: 17) ¡

((**n** x **a**) x **b**) = **n** ,! 19 (=E: 16,18) ¡

(((**n** x **a**) x **b**) = **n** ⇒ (**n** x (**a** x **b**)) = **n**)
,! 20 (∀E: V8.29) ¡

((**n** x **a**) x **b**) = **n** ⇒ (**n** x (**a** x **b**)) = **n**
,! 21 ()E: 20) ¡

(**n** x (**a** x **b**)) = **n** ,! 22 (⇒E: 19,21) ¡

(**n** x (**a** x **b**)) = **n** & ¬ **n** = 0 ,! 23 (&I: 14,22) ¡

ω[**n**] & ω[(**a** x **b**)] ,! 24 (𝕋E: V7.9,22) ¡

ω[**n**] ,! 25 (&E: 24) ¡

ω[(**a** x **b**)] ,! 26 (&E: 24) ¡

ω[**a**] & ω[**b**] ,! 27 (𝕋E: V7.9,26) ¡

((**n** x (**a** x **b**)) = **n** & ¬ **n** = 0 ⇒ (**a** x **b**) = 1)
,! 28 (∀E: V8.46;
(**a** x **b**): V7.9,27) ¡

(**n** x (**a** x **b**)) = **n** & ¬ **n** = 0 ⇒ (**a** x **b**) = 1
,! 29 ()E: 28) ¡

(**a** x **b**) = 1 ,! 30 (⇒E: 23,29) ¡

((**a** x **b**) = 1 ⇒ **a** = 1) ,! 31 (∀E: V8.63) ¡

(**a** x **b**) = 1 ⇒ **a** = 1 ,! 32 ()E: 31) ¡

a = 1 ,! 33 (⇒E: 30,32) ¡

(ω[**n**] ⇒ (**n** x 1) = **n**) ,! 34 (∀E: V8.18) ¡

ω[**n**] ⇒ (**n** x 1) = **n** ,! 35 ()E: 34) ¡

(**n** x 1) = **n** ,! 36 (⇒E: 25,35) ¡

(**n** x **a**) = **n** ,! 37 (=E: 33,36) ¡

n = **m** ,! 38 (=E: 16,37) ¡

¬ **n** = 0 ⇒ **n** = **m** ,! 39 (⇒I: 14,38) ¡

n = **m** ,! 40 (∨E: 6,13,39) ¡

n|**m** & **m**|**n** ⇒ **n** = **m** ,! 41 (⇒I: 2,40) ¡

(**n**|**m** & **m**|**n** ⇒ **n** = **m**) ,! 42 ()I: 41) ¡

∀n∀m∀k (n|m & m|n ⇒ n = m) ! 43 (∀I: 1,42) ¡

□

! **24. Transitivity of Division.** ¡

⊢ ∀n∀m∀k (n|m & m|k ⇒ n|k) ¡

	n,**m**,**k**	,! 1 (Prem) ¡
	n|**m** & **m**|**k**	,! 2 (Prem) ¡
	n|**m**	,! 3 (&E: 2) ¡
	m|**k**	,! 4 (&E: 2) ¡
	∃x (**n** x x) = **m**	,! 5 (𝕊E: P1,3) ¡
	(**n** x **a**) = **m**	,! 6 (∃E: 5) ¡
	∃x (**m** x x) = **k**	,! 7 (𝕊E: P1,4) ¡
	(**m** x **b**) = **k**	,! 8 (∃E: 7) ¡
	((**n** x **a**) x **b**) = **k**	,! 9 (=E: 6,8) ¡
	(((**n** x **a**) x **b**) = **k** ⇒ (**n** x (**a** x **b**)) = **k**)	,! 10 (∀E: V8.29) ¡
	((**n** x **a**) x **b**) = **k** ⇒ (**n** x (**a** x **b**)) = **k**	,! 11 (()E: 10) ¡
	(**n** x (**a** x **b**)) = **k**	,! 12 (⇒E: 9,11) ¡
	ω[**n**] & ω[(**a** x **b**)]	,! 13 (𝕋E: V7.9,12) ¡
	ω[(**a** x **b**)]	,! 14 (&E: 13) ¡
	ω[**a**] & ω[**b**]	,! 15 (𝕋E: V7.9,14) ¡
	∃x (**n** x x) = **k**	,! 16 (∃I: 15; (**a** x **b**): V7.9,15) ¡
	n|**k**	,! 17 (𝕊I: P1,16) ¡
	n|**m** & **m**|**k** ⇒ **n**|**k**	,! 18 (⇒I: 2,17) ¡
	(**n**|**m** & **m**|**k** ⇒ **n**|**k**)	,! 19 (()I: 18) ¡
∀n∀m∀k (n|m & m|k ⇒ n|k)		! 20 (∀I: 1,19) ¡

□

! P25-P30 show that division is maintained in additive and subtracting linear combinations. ¡

! **25.** ¡

```
⊢ ∀n∀m∀k ( n|m & n|k ⇒ n|(m + k) )                                  ¡
  n,m,k                                          ,! 1 (Prem)        ¡
    n|m & n|k                                    ,! 2 (Prem)        ¡
    n|m                                          ,! 3 (&E: 2)       ¡
    n|k                                          ,! 4 (&E: 2)       ¡
    ∃x (n x x) = m                               ,! 5 (𝕊E: V7.9,3)  ¡
    (n x a) = m                                  ,! 6 (∃E: 5)       ¡
    ∃x (n x x) = k                               ,! 7 (𝕊E: V7.9,4)  ¡
    (n x b) = k                                  ,! 8 (∃E: 7)       ¡
    ( ω[n] & ω[a] & ω[b]
      ⇒ (n x (a + b)) = ((n x a) + (n x b)) )
                                                 ,! 9 (∀E: V8.20)   ¡
    ω[n] & ω[a] & ω[b] ⇒ (n x (a + b)) = ((n x a) + (n x b))
                                                 ,! 10 (()E: 9)     ¡
    ω[n] & ω[a]                                  ,! 11 (𝕋E: V7.9,6) ¡
    ω[n] & ω[b]                                  ,! 12 (𝕋E: V7.9,8) ¡
    ω[a]                                         ,! 13 (&E: 11)     ¡
    ω[b]                                         ,! 14 (&E: 12)     ¡
    ω[n] & ω[a] & ω[b]                           ,! 15 (&I: 11,14)  ¡
    (n x (a + b)) = ((n x a) + (n x b))          ,! 16 (⇒E: 10,15)  ¡
    (n x (a + b)) = (m + (n x b))                ,! 17 (=E: 6,16)   ¡
    (n x (a + b)) = (m + k)                      ,! 18 (=E: 8,17)   ¡
    ω[a] & ω[b]                                  ,! 19 (&I: 13,14)  ¡
    ∃x (n x x) = (m + k)                         ,! 20 (∃I: 18;
                                                 (a + b): V1.7,19)  ¡
    n|(m + k)                                    ,! 21 (𝕊I: P1,20)  ¡
  n|m & n|k ⇒ n|(m + k)                          ,! 22 (⇒I: 2,21)   ¡
  ( n|m & n|k ⇒ n|(m + k) )                      ,! 23 (()I: 22)    ¡
∀n∀m∀k ( n|m & n|k ⇒ n|(m + k) )                   ! 24 (∀I: 1,23)   ¡
□
```

! **26.** ¡

⊢ ∀n∀m∀k (n|m & n|k & ≤[k,m] ⇒ n|(m - k)) ¡

n,**m**,**k** ,! 1 (Prem) ¡

n|**m** & **n**|**k** & ≤[**k**,**m**] ,! 2 (Prem) ¡

n|**m** ,! 3 (&E: 2) ¡

n|**k** ,! 4 (&E: 2) ¡

≤[**k**,**m**] ,! 5 (&E: 2) ¡

(**n** = 0 ∨ ¬ **n** = 0) ,! 6 (∀E: I3.4) ¡

n = 0 ∨ ¬ **n** = 0 ,! 7 ()E: 6) ¡

n = 0 ,! 8 (Prem) ¡

0|**m** ,! 9 (=E: 3,8) ¡

(0|**m** ⇒ **m** = 0) ,! 10 (∀E: P12) ¡

0|**m** ⇒ **m** = 0 ,! 11 ()E: 10) ¡

m = 0 ,! 12 (⇒E: 9,11) ¡

(**m** - 0) = 0 ,! 13 (=E: V6.18,12) ¡

0|**k** ,! 14 (=E: 4,8) ¡

(0|**k** ⇒ **k** = 0) ,! 15 (∀E: P12) ¡

0|**k** ⇒ **k** = 0 ,! 16 ()E: 15) ¡

k = 0 ,! 17 (⇒E: 14,16) ¡

(**m** - **k**) = 0 ,! 18 (=E: 13,17) ¡

(**m** - **k**) = **m** ,! 19 (=E: 12,18) ¡

n|(**m** - **k**) ,! 20 (=E: 3,19) ¡

n = 0 ⇒ **n**|(**m** - **k**) ,! 21 (⇒I: 8,20) ¡

¬ **n** = 0 ,! 22 (Prem) ¡

∃x (**n** x x) = **m** ,! 23 (∃E: P1,3) ¡

(**n** x **a**) = **m** ,! 24 (∃E: 23) ¡

≤[**k**,(**n** x **a**)] ,! 25 (=E: 5,25) ¡

∃x (**n** x x) = **k** ,! 26 (∃E: P1,4) ¡

(**n** x **b**) = **k** ,! 27 (∃E: 26) ¡

≤[(**n** x **b**),(**n** x **a**)] ,! 28 (=E: 25,27) ¡

≤[(**n** x **b**),(**n** x **a**)] & ¬ **n** = 0 ,! 29 (&I: 22,28) ¡

(≤[(**n** x **b**),(**n** x **a**)] & ¬ **n** = 0 ⇒ ≤[**b**,**a**])
,! 30 (∀E: V8.60) ¡

≤[(**n** x **b**),(**n** x **a**)] & ¬ **n** = 0 ⇒ ≤[**b**,**a**]
,! 31 ()E: 30) ¡

≤[**b**,**a**] ,! 32 (⇒E: 29,31) ¡

ω[**n**] & ω[**a**] ,! 33 (𝕋E: V7.9,28) ¡

ω[**n**] ,! 34 (&E: 33) ¡

≤[**b**,**a**] & ω[**n**] ,! 35 (&I: 32,34) ¡

(≤[**b**,**a**] & ω[**n**] ⇒ (**n** x (**a** - **b**)) = ((**n** x **a**) - (**n** x **b**)))
,! 36 (∀E: V8.36) ¡

≤[**b**,**a**] & ω[**n**] ⇒ (**n** x (**a** - **b**)) = ((**n** x **a**) - (**n** x **b**))
,! 37 ()E: 36) ¡

(**n** x (**a** - **b**)) = ((**n** x **a**) - (**n** x **b**))
,! 38 (⇒E: 35,37) ¡

(**n** x (**a** - **b**)) = (**m** - (**n** x **b**)) ,! 39 (=E: 24,38) ¡

(**n** x (**a** - **b**)) = (**m** - **k**) ,! 40 (=E: 27,39) ¡

∃x (**n** x x) = (**m** - **k**) ,! 41 (∃I: 40;
(**a** - **b**): V5.7,32) ¡

n|(**m** - **k**) ,! 42 (𝕊I: P1,41) ¡

¬ **n** = 0 ⇒ **n**|(**m** - **k**) ,! 43 (⇒I: 22,42) ¡

n|(**m** - **k**) ,! 44 (∨E: 7,21,43) ¡

n|**m** & **n**|**k** & ≤[**k**,**m**] ⇒ **n**|(**m** - **k**) ,! 45 (⇒I: 2,44) ¡

(**n**|**m** & **n**|**k** & ≤[**k**,**m**] ⇒ **n**|(**m** - **k**)) ,! 46 ()I: 45) ¡

∀n∀m∀k (n|m & n|k & ≤[k,m] ⇒ n|(m - k))
! 47 (∀I: 1,46) ¡

□

! **27.** ¡

⊢ ∀n∀m∀k (n|m & ω[k] ⇒ n|(m x k)) ¡

n,**m**,**k**	,! 1 (Prem)	¡
n|**m** & ω[**k**]	,! 2 (Prem)	¡
n|**m**	,! 3 (&E: 2)	¡
ω[**k**]	,! 4 (&E: 2)	¡
(**n**|**m** ⇒ ω[**m**])	,! 5 (∀E: P4)	¡
n|**m** ⇒ ω[**m**]	,! 6 (()E: 5)	¡
ω[**m**]	,! 7 (⇒E: 3,6)	¡
ω[**m**] & ω[**k**]	,! 8 (&E: 4,7)	¡
(ω[**m**] & ω[**k**] ⇒ **m**|(**m** x **k**))	,! 9 (∀E: P8)	¡
ω[**m**] & ω[**k**] ⇒ **m**|(**m** x **k**)	,! 10 (()E: 9)	¡
m|(**m** x **k**)	,! 11 (⇒E: 8,10)	¡
n|**m** & **m**|(**m** x **k**)	,! 12 (&I: 3,11)	¡
(**n**|**m** & **m**|(**m** x **k**) ⇒ **n**|(**m** x **k**))	,! 13 (∀E: P24; (**m** x **k**): V7.9,8)	¡
n|**m** & **m**|(**m** x **k**) ⇒ **n**|(**m** x **k**)	,! 14 (()E: 13)	¡
n|(**m** x **k**)	,! 15 (⇒E: 12,14)	¡
n|**m** & ω[**k**] ⇒ **n**|(**m** x **k**)	,! 16 (⇒I: 2,15)	¡
(**n**|**m** & ω[**k**] ⇒ **n**|(**m** x **k**))	,! 17 (()I: 16)	¡
∀n∀m∀k (n|m & ω[k] ⇒ n|(m x k))	! 18 (∀I: 1,17)	¡

□

! **28.** ¡

⊢ ∀n∀m∀k (n|m & ω[k] ⇒ n|(k x m)) ¡

n,**m**,**k**	,! 1 (Prem)	¡
n|**m** & ω[**k**]	,! 2 (Prem)	¡
(**n**|**m** & ω[**k**] ⇒ **n**|(**m** x **k**))	,! 3 (∀E: P27)	¡
n|**m** & ω[**k**] ⇒ **n**|(**m** x **k**)	,! 4 (()E: 3)	¡
n|(**m** x **k**)	,! 5 (⇒E: 2,4)	¡
∃x (**n** x x) = (**m** x **k**)	,! 6 (∃E: P1,5)	¡

(**n** x **x**) = (**m** x **k**) ,! 7 (∃E: 6) ¡

ω[**m**] & ω[**k**] ,! 8 (𝕋E: V7.9,7) ¡

(ω[**m**] & ω[**k**] ⇒ (**m** x **k**) = (**k** x **m**)) ,! 9 (∀E: V8.25) ¡

ω[**m**] & ω[**k**] ⇒ (**m** x **k**) = (**k** x **m**) ,! 10 (()E: 9) ¡

(**m** x **k**) = (**k** x **m**) ,! 11 (⇒E: 8,10) ¡

n|(**k** x **m**) ,! 12 (=E: 5,11) ¡

n|**m** & ω[**k**] ⇒ **n**|(**k** x **m**) ,! 13 (⇒I: 2,12) ¡

(**n**|**m** & ω[**k**] ⇒ **n**|(**k** x **m**)) ,! 14 (()I: 13) ¡

∀n∀m∀k (n|m & ω[k] ⇒ n|(k x m)) ! 15 (∀I: 1,14) ¡

□

! **29.** ¡

⊢ ∀n∀a∀b∀x∀y (n|x & n|y & ω[a] & ω[b] ⇒ n|((axx) + (bxy))) ¡

n,**a**,**b**,**x**,**y** ,! 1 (Prem) ¡

n|**x** & **n**|**y** & ω[**a**] & ω[**b**] ,! 2 (Prem) ¡

n|**x** ,! 3 (&E: 2) ¡

n|**y** ,! 4 (&E: 2) ¡

ω[**a**] ,! 5 (&E: 2) ¡

ω[**b**] ,! 6 (&E: 2) ¡

n|**x** & ω[**a**] ,! 7 (&I: 3,5) ¡

(**n**|**x** & ω[**a**] ⇒ **n**|(**a** x **x**)) ,! 8 (∀E: P28) ¡

n|**x** & ω[**a**] ⇒ **n**|(**a** x **x**) ,! 9 (()E: 8) ¡

n|(**a** x **x**) ,! 10 (⇒E: 7,9) ¡

n|**y** & ω[**b**] ,! 11 (&I: 4,6) ¡

(**n**|**y** & ω[**b**] ⇒ **n**|(**b** x **y**)) ,! 12 (∀E: P28) ¡

n|**y** & ω[**b**] ⇒ **n**|(**b** x **y**) ,! 13 (()E: 12) ¡

n|(**b** x **y**) ,! 14 (⇒E: 11,13) ¡

n|(**a** x **x**) & **n**|(**b** x **y**) ,! 15 (&I: 10,14) ¡

(**n**|**x** ⇒ ω[**x**]) ,! 16 (∀E: P4) ¡

n|**x** ⇒ ω[**x**] ,! 17 (()E: 16) ¡

ω[**x**] ,! 18 (⇒E: 3,17) ¡

ω[**a**] & ω[**x**] ,! 19 (&I: 5,18) ¡

(**n**|**y** ⇒ ω[**y**]) ,! 20 (∀E: P4) ¡

n|**y** ⇒ ω[**y**] ,! 21 (()E: 20) ¡

ω[**y**] ,! 22 (⇒E: 4,21) ¡

ω[**b**] & ω[**y**] ,! 23 (&E: 6,22) ¡

(**n**|(**a** x **x**) & **n**|(**b** x **y**) ⇒ **n**|((**a** x **x**) + (**b** x **y**)))
,! 24 (∀E: P25;
(**a** x **x**): V7.9,19;
(**b** x **y**): V7.9,23) ¡

n|(**a** x **x**) & **n**|(**b** x **y**) ⇒ **n**|((**a** x **x**) + (**b** x **y**))
,! 25 (()E: 24) ¡

n|((**a** x **x**) + (**b** x **y**)) ,! 26 (⇒E: 15,25) ¡

n|**x** & **n**|**y** & ω[**a**] & ω[**b**] ⇒ **n**|((**a** x **x**) + (**b** x **y**))
,! 27 (⇒I: 2,26) ¡

(**n**|**x** & **n**|**y** & ω[**a**] & ω[**b**] ⇒ **n**|((**a** x **x**) + (**b** x **y**)))
,! 28 (()I: 27) ¡

∀n∀a∀b∀x∀y (n|x & n|y & ω[a] & ω[b] ⇒ n|((axx) + (bxy)))
! 29 (∀I: 1,28) ¡

□

! **30.** ¡

⊢ ∀n∀a∀b∀x∀y (n|x & n|y & ≤[(bxy),(axx)] ⇒ n|((axx) - (bxy)))
¡

n,**a**,**b**,**x**,**y** ,! 1 (Prem) ¡

n|**x** & **n**|**y** & ≤[(**b**x**y**),(**a**x**x**)] ,! 2 (Prem) ¡

n|**x** ,! 3 (&E: 2) ¡

n|**y** ,! 4 (&E: 2) ¡

≤[(**b**x**y**),(**a**x**x**)] ,! 5 (&E: 2) ¡

ω[**a**] & ω[**x**] ,! 6 (𝕋E: V7.9,5) ¡

ω[**b**] & ω[**y**] ,! 7 (𝕋E: V7.9,5) ¡

ω[**a**] ,! 8 (&E: 6) ¡

n|**x** & ω[**a**] ,! 9 (&I: 3,8) ¡

(**n**|**x** & ω[**a**] ⇒ **n**|(**a** x **x**)) ,! 10 (∀E: P28) ¡

n|**x** & ω[**a**] ⇒ **n**|(**a** x **x**) ,! 11 (()E: 10) ¡

n|(**a** x **x**) ,! 12 (⇒E: 9,11) ¡

n|(**a** x **x**) & ≤[(**b**x**y**),(**a**x**x**)] ,! 13 (&I: 5,12) ¡

ω[**b**] ,! 14 (&E: 7) ¡

n|**y** & ω[**b**] ,! 15 (&I: 4,14) ¡

(**n**|**y** & ω[**b**] ⇒ **n**|(**b** x **y**)) ,! 16 (∀E: P28) ¡

n|**y** & ω[**b**] ⇒ **n**|(**b** x **y**) ,! 17 (()E: 16) ¡

n|(**b** x **y**) ,! 18 (⇒E: 15,17) ¡

n|(**a** x **x**) & **n**|(**b** x **y**) & ≤[(**b**x**y**),(**a**x**x**)]
,! 19 (&I: 13,18) ¡

(**n**|(**a** x **x**) & **n**|(**b** x **y**) & ≤[(**b**x**y**),(**a**x**x**)]
⇒ **n**|((**a**x**x**) - (**b**x**y**)))
,! 20 (∀E: P26;
(**a** x **x**): V7.9,6;
(**b** x **y**): V7.9,7) ¡

n|(**a** x **x**) & **n**|(**b** x **y**) & ≤[(**b**x**y**),(**a**x**x**)]
⇒ **n**|((**a**x**x**) - (**b**x**y**))
,! 21 (()E: 20 ¡

n|((**a** x **x**) - (**b** x **y**)) ,! 22 (⇒E: 19,21) ¡

n|**x** & **n**|**y** & ≤[(**b**x**y**),(**a**x**x**)] ⇒ **n**|((**a** x **x**) - (**b** x **y**))
,! 23 (⇒I: 2,22) ¡

(**n**|**x** & **n**|**y** & ≤[(**b**x**y**),(**a**x**x**)] ⇒ **n**|((**a** x **x**) - (**b** x **y**)))
,! 24 (()I: 23) ¡

∀n∀a∀b∀x∀y (n|x & n|y & ≤[(bxy),(axx)] ⇒ n|((axx) - (bxy)))
! 25 (∀I: 1,24) ¡

□

! P31-P46 are various permutations on the theme that division of both the sum (or difference) and one of the terms implies division of the other term. ¡

! **31.** ¡

⊢ ∀n∀m∀k (n|(m + k) & n|m ⇒ n|k)

n,**m**,**k** ,! 1 (Prem)

n|(**m** + **k**) & **n**|**m** ,! 2 (Prem)

n|(**m** + **k**) ,! 3 (&E: 2)

∃x (**n** x x) = (**m** + **k**) ,! 4 (𝕊E: P1,3)

(**n** x **x**) = (**m** + **k**) ,! 5 (∃E: 4)

ω[**m**] & ω[**k**] ,! 6 (𝕋E: V1.7,5)

(ω[**m**] & ω[**k**] ⇒ ≤[**m**,(**m** + **k**)]) ,! 7 (∀E: V3.33)

ω[**m**] & ω[**k**] ⇒ ≤[**m**,(**m** + **k**)] ,! 8 ()E: 7)

≤[**m**,(**m** + **k**)] ,! 9 (⇒E: 6,8)

n|(**m** + **k**) & **n**|**m** & ≤[**m**,(**m** + **k**)] ,! 10 (&I: 2,9)

(**n**|(**m** + **k**) & **n**|**m** & ≤[**m**,(**m** + **k**)] ⇒ **n**|((**m** + **k**) - **m**))
,! 11 (∀E: P26;
(**m** + **k**): V1.7,6)

n|(**m** + **k**) & **n**|**m** & ≤[**m**,(**m** + **k**)] ⇒ **n**|((**m** + **k**) - **m**)
,! 12 ()E: 11)

n|((**m** + **k**) - **m**) ,! 13 (⇒E: 10,12)

(ω[**m**] & ω[**k**] ⇒ ((**m** + **k**) - **m**) = **k**) ,! 14 (∀E: V6.36)

ω[**m**] & ω[**k**] ⇒ ((**m** + **k**) - **m**) = **k** ,! 15 ()E: 14)

((**m** + **k**) - **m**) = **k** ,! 16 (⇒E: 6,15)

n|**k** ,! 17 (=E: 13,16)

n|(**m** + **k**) & **n**|**m** ⇒ **n**|**k** ,! 18 (⇒I: 2,17)

(**n**|(**m** + **k**) & **n**|**m** ⇒ **n**|**k**) ,! 19 ()I: 18)

∀n∀m∀k (n|(m + k) & n|m ⇒ n|k) ! 20 (∀I: 1,19)

□

! **32.**

⊢ ∀n∀m∀k (n|(m + k) & n|k ⇒ n|m)

n,**m**,**k** ,! 1 (Prem)

n|(**m** + **k**) & **n**|**k** ,! 2 (Prem)

n|(**m** + **k**) ,! 3 (&E: 2)

n|**k** ,! 4 (&E: 2) ¡

∃x (**n** x x) = (**m** + **k**) ,! 5 (𝕊E: P1,3) ¡

(**n** x **x**) = (**m** + **k**) ,! 6 (∃E: 5) ¡

ω[**m**] & ω[**k**] ,! 7 (𝕋E: V1.7,6) ¡

(ω[**m**] & ω[**k**] ⇒ (**m** + **k**) = (**k** + **m**)) ,! 8 (∀E: V2.5) ¡

ω[**m**] & ω[**k**] ⇒ (**m** + **k**) = (**k** + **m**) ,! 9 (()E: 8) ¡

(**m** + **k**) = (**k** + **m**) ,! 10 (⇒E: 7,9) ¡

n|(**k** + **m**) ,! 11 (=E: 3,10) ¡

n|(**k** + **m**) & **n**|**k** ,! 12 (&I: 4,11) ¡

(**n**|(**k** + **m**) & **n**|**k** ⇒ **n**|**m**) ,! 13 (∀E: P31) ¡

n|(**k** + **m**) & **n**|**k** ⇒ **n**|**m** ,! 14 (()E: 13) ¡

n|**m** ,! 15 (⇒E: 12,14) ¡

n|(**m** + **k**) & **n**|**k** ⇒ **n**|**m** ,! 16 (⇒I: 2,15) ¡

(**n**|(**m** + **k**) & **n**|**k** ⇒ **n**|**m**) ,! 17 (()I: 16) ¡

∀n∀m∀k (n|(m + k) & n|k ⇒ n|m) ! 18 (∀I: 1,17) ¡

□

! **33.** ¡

⊢ ∀n∀m∀k (n|(m - k) & n|k ⇒ n|m) ¡

n,**m**,**k** ,! 1 (Prem) ¡

n|(**m** - **k**) & **n**|**k** ,! 2 (Prem) ¡

n|(**m** - **k**) ,! 3 (&E: 2) ¡

∃x (**n** x x) = (**m** - **k**) ,! 4 (𝕊E: P1,3) ¡

(**n** x **x**) = (**m** - **k**) ,! 5 (∃E: 4) ¡

≤[**k**,**m**] ,! 6 (𝕋E: V5.7,5) ¡

(**n**|(**m** - **k**) & **n**|**k** ⇒ **n**|((**m** - **k**) + **k**)) ,! 7 (∀E: P25; (**m** - **k**): V5.7,5) ¡

n|(**m** - **k**) & **n**|**k** ⇒ **n**|((**m** - **k**) + **k**) ,! 8 (()E: 7) ¡

n|((**m** - **k**) + **k**) ,! 9 (⇒E: 2,8) ¡

```
    ( ≤[k,m] ⇒ ((m - k) + k) = m )        ,! 10 (∀E: V6.3)    ¡
    ≤[k,m] ⇒ ((m - k) + k) = m            ,! 11 (()E: 10)     ¡
    ((m - k) + k) = m                     ,! 12 (⇒E: 6,11)    ¡
    n|m                                   ,! 13 (=E: 9,12)    ¡
  n|(m - k) & n|k ⇒ n|m                   ,! 14 (⇒I: 2,13)    ¡
  ( n|(m - k) & n|k ⇒ n|m )                ,! 15 (()I: 14)     ¡
∀n∀m∀k ( n|(m - k) & n|k ⇒ n|m )            ! 16 (∀I: 1,15)    ¡
□
! 34.                                                          ¡
⊢ ∀n∀m∀k ( n|(m - k) & n|m ⇒ n|k )                             ¡
  n,m,k                                   ,! 1 (Prem)         ¡
    n|(m - k) & n|m                       ,! 2 (Prem)         ¡
    n|(m - k)                             ,! 3 (&E: 2)        ¡
    n|m                                   ,! 4 (&E: 2)        ¡
    ∃x (n x x) = (m - k)                  ,! 5 (𝕊E: P1,3)     ¡
    (n x a) = (m - k)                     ,! 6 (∃E: 5)        ¡
    ≤[k,m]                                ,! 7 (𝕋E: V5.7,6)   ¡
    ( ≤[k,m] ⇒ (m - (m - k)) = k )        ,! 8 (∀E: V6.37)    ¡
    ≤[k,m] ⇒ (m - (m - k)) = k            ,! 9 (()E: 8)       ¡
    (m - (m - k)) = k                     ,! 10 (⇒E: 7,9)     ¡
    ( n|m & n|(m - k) & ≤[(m - k),m] ⇒ n|(m - (m - k)) )
                                          ,! 11 (∀E: P26;
                                          (m - k): V5.7,7)    ¡
    n|m & n|(m - k) & ≤[(m - k),m] ⇒ n|(m - (m - k))
                                          ,! 12 (()E: 11)     ¡
    n|m & n|(m - k)                       ,! 13 (&I: 3,4)     ¡
    ≤[(m - k),m]                          ,! 14 (𝕋E: V5.7,10) ¡
    n|m & n|(m - k) & ≤[(m - k),m]        ,! 15 (&I: 13,14)   ¡
    n|(m - (m - k))                       ,! 16 (⇒E: 11,15)   ¡
    n|k                                   ,! 17 (=E: 10,16)   ¡
```

n|(**m** - **k**) & **n**|**m** ⇒ **n**|**k** ,! 18 (⇒I: 2,17) ¡

(**n**|(**m** - **k**) & **n**|**m** ⇒ **n**|**k**) ,! 19 (()I: 18) ¡

∀n∀m∀k (n|(m - k) & n|m ⇒ n|k) ! 20 (∀I: 1,19) ¡

□

! **35.** ¡

⊢ ∀a∀b∀c∀n (a = (b + c) & n|b & n|c ⇒ n|a) ¡

a,**b**,**c**,**n** ,! 1 (Prem) ¡

a = (**b** + **c**) & **n**|**b** & **n**|**c** ,! 2 (Prem) ¡

a = (**b** + **c**) ,! 3 (&E: 2) ¡

n|**b** & **n**|**c** ,! 4 (&E: 2) ¡

(**n**|**b** & **n**|**c** ⇒ **n**|(**b** + **c**)) ,! 5 (∀E: P25) ¡

n|**b** & **n**|**c** ⇒ **n**|(**b** + **c**) ,! 6 (()E: 5) ¡

n|(**b** + **c**) ,! 7 (⇒E: 4,6) ¡

n|**a** ,! 8 (=E: 3,7) ¡

a = (**b** + **c**) & **n**|**b** & **n**|**c** ⇒ **n**|**a** ,! 9 (⇒I: 2,8) ¡

(**a** = (**b** + **c**) & **n**|**b** & **n**|**c** ⇒ **n**|**a**) ,! 10 (()I: 9) ¡

∀a∀b∀c∀n (a = (b + c) & n|b & n|c ⇒ n|a)
! 11 (∀I: 1,10) ¡

□

! **36.** P36 is proved here implicitly as a corollary of P41. The present organization has been chosen in order to group like-looking propositions. ¡

⊢ ∀a∀b∀c∀n (a = (b + c) & n|a & n|b ⇒ n|c) ¡

a,**b**,**c**,**n** ,! 1 (Prem) ¡

a = (**b** + **c**) & **n**|**a** & **n**|**b** ,! 2 (Prem) ¡

a = (**b** + **c**) ,! 3 (&E: 2) ¡

n|**a** & **n**|**b** ,! 4 (&E: 2) ¡

(**a** = (**b** + **c**) ⇒ **c** = (**a** - **b**)) ,! 5 (∀E: V6.13) ¡

a = (**b** + **c**) ⇒ **c** = (**a** - **b**) ,! 6 (()E: 5) ¡

c = (**a** - **b**) ,! 7 (⇒E: 3,6) ¡

```
    ≤[b,a]                                  ,! 8 (𝕋E: V5.7,7)   ¡
    n|a & n|b & ≤[b,a]                      ,! 9 (&I: 7,8)      ¡
    ( n|a & n|b & ≤[b,a] ⇒ n|(a - b) )      ,! 10 (∀E: P26)     ¡
    n|a & n|b & ≤[b,a] ⇒ n|(a - b)          ,! 11 (()E: 10)     ¡
    n|(a - b)                               ,! 12 (⇒E: 9,11)    ¡
    n|c                                     ,! 13 (=E: 7,12)    ¡
  a = (b + c) & n|a & n|b ⇒ n|c             ,! 14 (⇒I: 2,13)    ¡
  ( a = (b + c) & n|a & n|b ⇒ n|c )         ,! 15 (()I: 14)     ¡
∀a∀b∀c∀n ( a = (b + c) & n|a & n|b ⇒ n|c )
                                            ! 16 (∀I: 1,15)     ¡
□
! 37.                                                           ¡
⊢ ∀a∀b∀c∀n ( a = (b + c) & n|a & n|c ⇒ n|b )                    ¡
  a,b,c,n                                   ,! 1 (Prem)         ¡
    a = (b + c) & n|a & n|c                 ,! 2 (Prem)         ¡
    a = (b + c)                             ,! 3 (&E: 2)        ¡
    n|a & n|c                               ,! 4 (&E: 2)        ¡
    ( a = (b + c) ⇒ a = (c + b) )           ,! 5 (∀E: V2.7)     ¡
    a = (b + c) ⇒ a = (c + b)               ,! 6 (()E: 5)       ¡
    a = (c + b)                             ,! 7 (⇒E: 3,6)      ¡
    a = (c + b) & n|a & n|c                 ,! 8 (&I: 4,7)      ¡
    ( a = (c + b) & n|a & n|c ⇒ n|b )       ,! 9 (∀E: P36)      ¡
    a = (c + b) & n|a & n|c ⇒ n|b           ,! 10 (()E: 9)      ¡
    n|b                                     ,! 11 (⇒E: 8,10)    ¡
  a = (b + c) & n|a & n|c ⇒ n|b             ,! 12 (⇒I: 2,11)    ¡
  ( a = (b + c) & n|a & n|c ⇒ n|b )         ,! 13 (()I: 12)     ¡
∀a∀b∀c∀n ( a = (b + c) & n|a & n|c ⇒ n|b )
                                            ! 14 (∀I: 1,13)     ¡
□
```

! **38.** ¡

⊢ ∀a∀b∀c∀n ((b + c) = a & n|b & n|c ⇒ n|a) ¡

a,**b**,**c**,**n** ,! 1 (Prem) ¡

(**b** + **c**) = **a** & **n**|**b** & **n**|**c** ,! 2 (Prem) ¡

(**b** + **c**) = **a** ,! 3 (&E: 2) ¡

n|**b** & **n**|**c** ,! 4 (&E: 2) ¡

a = **a** ,! 5 (=I) ¡

a = (**b** + **c**) ,! 6 (=E: 3,5) ¡

a = (**b** + **c**) & **n**|**b** & **n**|**c** ,! 7 (&I: 4,6) ¡

(**a** = (**b** + **c**) & **n**|**b** & **n**|**c** ⇒ **n**|**a**) ,! 8 (∀E: P35) ¡

a = (**b** + **c**) & **n**|**b** & **n**|**c** ⇒ **n**|**a** ,! 9 (()E: 8) ¡

n|**a** ,! 10 (⇒E: 7,9) ¡

(**b** + **c**) = **a** & **n**|**b** & **n**|**c** ⇒ **n**|**a** ,! 11 (⇒I: 2,10) ¡

((**b** + **c**) = **a** & **n**|**b** & **n**|**c** ⇒ **n**|**a**) ,! 12 (()I: 11) ¡

∀a∀b∀c∀n ((b + c) = a & n|b & n|c ⇒ n|a)
! 13 (∀I: 1,12) ¡

□

! **39.** ¡

⊢ ∀a∀b∀c∀n ((b + c) = a & n|a & n|b ⇒ n|c) ¡

a,**b**,**c**,**n** ,! 1 (Prem) ¡

(**b** + **c**) = **a** & **n**|**a** & **n**|**b** ,! 2 (Prem) ¡

(**b** + **c**) = **a** ,! 3 (&E: 2) ¡

n|**a** & **n**|**b** ,! 4 (&E: 2) ¡

a = **a** ,! 5 (=I) ¡

a = (**b** + **c**) ,! 6 (=E: 3,5) ¡

a = (**b** + **c**) & **n**|**a** & **n**|**b** ,! 7 (&I: 4,6) ¡

(**a** = (**b** + **c**) & **n**|**a** & **n**|**b** ⇒ **n**|**c**) ,! 8 (∀E: P36) ¡

a = (**b** + **c**) & **n**|**a** & **n**|**b** ⇒ **n**|**c** ,! 9 (()E: 8) ¡

n|**c** ,! 10 (⇒E: 7,9) ¡

(**b** + **c**) = **a** & **n**|**a** & **n**|**b** ⇒ **n**|**c** ,! 11 (⇒I: 2,10) ¡

((**b** + **c**) = **a** & **n**|**a** & **n**|**b** ⇒ **n**|**c**) ,! 12 (()I: 11) ¡

∀a∀b∀c∀n ((b + c) = a & n|a & n|b ⇒ n|c)
! 13 (∀I: 1,12) ¡

□

! **40.** ¡

⊢ ∀a∀b∀c∀n ((b + c) = a & n|a & n|c ⇒ n|b) ¡

a,**b**,**c**,**n** ,! 1 (Prem) ¡

(**b** + **c**) = **a** & **n**|**a** & **n**|**c** ,! 2 (Prem) ¡

(**b** + **c**) = **a** ,! 3 (&E: 2) ¡

n|**a** & **n**|**c** ,! 4 (&E: 2) ¡

a = **a** ,! 5 (=I) ¡

a = (**b** + **c**) ,! 6 (=E: 3,5) ¡

a = (**b** + **c**) & **n**|**a** & **n**|**c** ,! 7 (=E: 4,6) ¡

(**a** = (**b** + **c**) & **n**|**a** & **n**|**c** ⇒ **n**|**b**) ,! 8 (∀E: P37) ¡

a = (**b** + **c**) & **n**|**a** & **n**|**c** ⇒ **n**|**b** ,! 9 (()E: 8) ¡

n|**b** ,! 10 (⇒E: 7,9) ¡

(**b** + **c**) = **a** & **n**|**a** & **n**|**c** ⇒ **n**|**b** ,! 11 (⇒I: 2,10) ¡

((**b** + **c**) = **a** & **n**|**a** & **n**|**c** ⇒ **n**|**b**) ,! 12 (()I: 11) ¡

∀a∀b∀c∀n ((b + c) = a & n|a & n|c ⇒ n|b)
! 13 (∀I: 1,12) ¡

□

! **41.** ¡

⊢ ∀a∀b∀c∀n (a = (b - c) & n|b & n|c ⇒ n|a) ¡

a,**b**,**c**,**n** ,! 1 (Prem) ¡

a = (**b** - **c**) & **n**|**b** & **n**|**c** ,! 2 (Prem) ¡

a = (**b** - **c**) ,! 3 (&E: 2) ¡

n|**b** & **n**|**c** ,! 4 (&E: 2) ¡

≤[**c**,**b**] ,! 5 (𝕋E: V5.7,3) ¡

n|**b** & **n**|**c** & ≤[**c**,**b**] ,! 6 (&I: 4,5) ¡

(**n**|**b** & **n**|**c** & ≤[**c**,**b**] ⇒ **n**|(**b** - **c**)) ,! 7 (∀E: P26) ¡

n|**b** & **n**|**c** & ≤[**c**,**b**] ⇒ **n**|(**b** - **c**) ,! 8 ()E: 7) ¡

n|(**b** - **c**) ,! 9 (⇒E: 6,8) ¡

n|**a** ,! 10 (=E: 3,9) ¡

a = (**b** - **c**) & **n**|**b** & **n**|**c** ⇒ **n**|**a** ,! 11 (⇒I: 2,10) ¡

(**a** = (**b** - **c**) & **n**|**b** & **n**|**c** ⇒ **n**|**a**) ,! 12 ()I: 11) ¡

∀a∀b∀c∀n (a = (b - c) & n|b & n|c ⇒ n|a)
,! 13 (∀I: 1,12) ¡

□

! **42.** ¡

⊢ ∀a∀b∀c∀n (a = (b - c) & n|a & n|b ⇒ n|c) ¡

a,**b**,**c**,**n** ,! 1 (Prem) ¡

a = (**b** - **c**) & **n**|**a** & **n**|**b** ,! 2 (Prem) ¡

a = (**b** - **c**) ,! 3 (&E: 2) ¡

n|**a** ,! 4 (&E: 2) ¡

n|**b** ,! 5 (&E: 2) ¡

(**a** = (**b** - **c**) ⇒ **b** = (**c** + **a**)) ,! 6 (∀E: V6.11) ¡

a = (**b** - **c**) ⇒ **b** = (**c** + **a**) ,! 7 ()E: 6) ¡

b = (**c** + **a**) ,! 8 (⇒E: 3,7) ¡

b = (**c** + **a**) & **n**|**b** ,! 9 (&I: 5,8) ¡

b = (**c** + **a**) & **n**|**b** & **n**|**a** ,! 10 (&I: 4,9) ¡

(**b** = (**c** + **a**) & **n**|**b** & **n**|**a** ⇒ **n**|**c**) ,! 11 (∀E: P37) ¡

b = (**c** + **a**) & **n**|**b** & **n**|**a** ⇒ **n**|**c** ,! 12 ()E: 11) ¡

n|**c** ,! 13 (⇒E: 10,12) ¡

a = (**b** - **c**) & **n**|**a** & **n**|**b** ⇒ **n**|**c** ,! 14 (⇒I: 2,13) ¡

(**a** = (**b** - **c**) & **n**|**a** & **n**|**b** ⇒ **n**|**c**) ,! 15 ()I: 14) ¡

∀a∀b∀c∀n (a = (b - c) & n|a & n|b ⇒ n|c)
,! 16 (∀I: 1,15) ¡

□

! **43.** ¡

⊢ ∀a∀b∀c∀n (a = (b - c) & n|a & n|c ⇒ n|b) ¡

a,b,c,n ,! 1 (Prem) ¡

a = (**b** - **c**) & **n**|**a** & **n**|**c** ,! 2 (Prem) ¡

a = (**b** - **c**) ,! 3 (&E: 2) ¡

n|**a** ,! 4 (&E: 2) ¡

n|**c** ,! 5 (&E: 2) ¡

(**a** = (**b** - **c**) ⇒ **b** = (**c** + **a**)) ,! 6 (∀E: V6.11) ¡

a = (**b** - **c**) ⇒ **b** = (**c** + **a**) ,! 7 (()E: 6) ¡

b = (**c** + **a**) ,! 8 (⇒E: 3,7) ¡

b = (**c** + **a**) & **n**|**c** ,! 9 (&I: 5,8) ¡

b = (**c** + **a**) & **n**|**c** & **n**|**a** ,! 10 (&I: 4,9) ¡

(**b** = (**c** + **a**) & **n**|**c** & **n**|**a** ⇒ **n**|**b**) ,! 11 (∀E: P35) ¡

b = (**c** + **a**) & **n**|**c** & **n**|**a** ⇒ **n**|**b** ,! 12 (()E: 11) ¡

n|**b** ,! 13 (⇒E: 10,12) ¡

a = (**b** - **c**) & **n**|**a** & **n**|**c** ⇒ **n**|**b** ,! 14 (⇒I: 2,13) ¡

(**a** = (**b** - **c**) & **n**|**a** & **n**|**c** ⇒ **n**|**b**) ,! 15 (()I: 14) ¡

∀a∀b∀c∀n (a = (b - c) & n|a & n|c ⇒ n|b)
! 16 (∀I: 1,15) ¡

□

! **44.** ¡

⊢ ∀a∀b∀c∀n ((b - c) = a & n|b & n|c ⇒ n|a) ¡

a,b,c,n ,! 1 (Prem) ¡

(**b** - **c**) = **a** & **n**|**b** & **n**|**c** ,! 2 (Prem) ¡

(**b** - **c**) = **a** ,! 3 (&E: 2) ¡

n|**b** & **n**|**c** ,! 4 (&E: 2) ¡

a = **a** ,! 5 (=I) ¡

a = (**b** - **c**) ,! 6 (=E: 3,5) ¡

a = (**b** - **c**) & **n**|**b** & **n**|**c** ,! 7 (=E: 4,6) ¡

(**a** = (**b** - **c**) & **n**|**b** & **n**|**c** ⇒ **n**|**a**) ,! 8 (∀E: P41) ¡

a = (**b** - **c**) & **n**|**b** & **n**|**c** ⇒ **n**|**a** ,! 9 (()E: 8) ¡

n|**a** ,! 10 (⇒E: 7,9) ¡

(**b** - **c**) = **a** & **n**|**b** & **n**|**c** ⇒ **n**|**a** ,! 11 (⇒I: 2,10) ¡

((**b** - **c**) = **a** & **n**|**b** & **n**|**c** ⇒ **n**|**a**) ,! 12 (()I: 11) ¡

∀a∀b∀c∀n ((b - c) = a & n|b & n|c ⇒ n|a)
,! 13 (∀I: 1,12) ¡

□

! **45.** ¡

⊢ ∀a∀b∀c∀n ((b - c) = a & n|a & n|b ⇒ n|c) ¡

a,**b**,**c**,**n** ,! 1 (Prem) ¡

(**b** - **c**) = **a** & **n**|**a** & **n**|**b** ,! 2 (Prem) ¡

(**b** - **c**) = **a** ,! 3 (&E: 2) ¡

n|**a** & **n**|**b** ,! 4 (&E: 2) ¡

a = **a** ,! 5 (=I) ¡

a = (**b** - **c**) ,! 6 (=E: 3,5) ¡

a = (**b** - **c**) & **n**|**a** & **n**|**b** ,! 7 (&I: 4,6) ¡

(**a** = (**b** - **c**) & **n**|**a** & **n**|**b** ⇒ **n**|**c**) ,! 8 (∀E: P42) ¡

a = (**b** - **c**) & **n**|**a** & **n**|**b** ⇒ **n**|**c** ,! 9 (()E: 8) ¡

n|**c** ,! 10 (⇒E: 7,9) ¡

(**b** - **c**) = **a** & **n**|**a** & **n**|**b** ⇒ **n**|**c** ,! 11 (⇒I: 2,10) ¡

((**b** - **c**) = **a** & **n**|**a** & **n**|**b** ⇒ **n**|**c**) ,! 12 (()I: 11) ¡

∀a∀b∀c∀n ((b - c) = a & n|a & n|b ⇒ n|c)
,! 13 (∀I: 1,12) ¡

□

! **46.** ¡

⊢ ∀a∀b∀c∀n ((b - c) = a & n|a & n|c ⇒ n|b) ¡

a,**b**,**c**,**n** ,! 1 (Prem) ¡

(**b** - **c**) = **a** & **n**|**a** & **n**|**c** ,! 2 (Prem) ¡

(**b** - **c**) = **a** ,! 3 (&E: 2) ¡

n|**a** & **n**|**c** ,! 4 (&E: 2) ¡

a = **a** ,! 5 (=I) ¡

a = (**b** - **c**) ,! 6 (=E: 3,5) ¡

a = (**b** - **c**) & **n**|**a** & **n**|**c** ,! 7 (&I: 4,6) ¡

(**a** = (**b** - **c**) & **n**|**a** & **n**|**c** ⇒ **n**|**b**) ,! 8 (∀E: P43) ¡

a = (**b** - **c**) & **n**|**a** & **n**|**c** ⇒ **n**|**b** ,! 9 (()E: 8) ¡

n|**b** ,! 10 (⇒E: 7,9) ¡

(**b** - **c**) = **a** & **n**|**a** & **n**|**c** ⇒ **n**|**b** ,! 11 (⇒I: 2,10) ¡

((**b** - **c**) = **a** & **n**|**a** & **n**|**c** ⇒ **n**|**b**) ,! 12 (()I: 11) ¡

∀a∀b∀c∀n ((b - c) = a & n|a & n|c ⇒ n|b)
,! 13 (∀I: 1,12) ¡

□

! **47.** ¡

⊢ ∀n∀m (n|m & ¬ m = 0 ⇒ ≤[n,m]) ¡

n,**m** ,! 1 (Prem) ¡

n|**m** & ¬ **m** = 0 ,! 2 (Prem) ¡

n|**m** ,! 3 (&E: 2) ¡

¬ **m** = 0 ,! 4 (&E: 2) ¡

∃x (**n** x x) = **m** ,! 5 (∃E: P1,3) ¡

(**n** x **x**) = **m** ,! 6 (∃E: 5) ¡

(**n** x **x**) = **m** & ¬ **m** = 0 ,! 7 (&I: 4,6) ¡

((**n** x **x**) = **m** & ¬ **m** = 0 ⇒ ¬ **x** = 0) ,! 8 (∀E: V8.9) ¡

(**n** x **x**) = **m** & ¬ **m** = 0 ⇒ ¬ **x** = 0 ,! 9 (()E: 8) ¡

¬ **x** = 0 ,! 10 (⇒E: 7,9) ¡

ω[**n**] & ω[**x**] ,! 11 (𝕋E: V7.9,6) ¡

ω[**n**] & ω[**x**] & ¬ **x** = 0 ,! 12 (&I: 10,11) ¡

(ω[**n**] & ω[**x**] & ¬ **x** = 0 ⇒ ≤[**n**,(**n** x **x**)])
,! 13 (∀E: V8.53) ¡

ω[**n**] & ω[**x**] & ¬ **x** = 0 ⇒ ≤[**n**,(**n** x **x**)] ,! 14 (()E: 13) ¡

≤[**n**,(**n** x **x**)] ,! 15 (⇒E: 12,14) ¡

≤[**n**,**m**] ,! 16 (=E: 6,15) ¡

n|**m** & ¬ **m** = 0 ⇒ ≤[**n**,**m**] ,! 17 (⇒I: 2,16) ¡

(**n**|**m** & ¬ **m** = 0 ⇒ ≤[**n**,**m**]) ,! 18 ()I: 17) ¡

∀n∀m (n|m & ¬ m = 0 ⇒ ≤[n,m]) ! 19 (∀I: 1,18) ¡

□

! **48.** Only 1 and 2 divide 2. ¡

⊢ ∀n (n|2 ⇒ n = 1 ∨ n = 2) ¡

n ,! 1 (Prem) ¡

n|2 ,! 2 (Prem) ¡

n|2 & ¬ 2 = 0 ,! 3 (&I: IV9.17) ¡

(**n**|2 & ¬ 2 = 0 ⇒ ≤[**n**,2]) ,! 4 (∀E: P47) ¡

n|2 & ¬ 2 = 0 ⇒ ≤[**n**,2] ,! 5 ()E: 4) ¡

≤[**n**,2] ,! 6 (⇒E: 3,5) ¡

(≤[**n**,2] ⇒ **n** = 0 ∨ **n** = 1 ∨ **n** = 2) ,! 7 (∀E: V3.59) ¡

≤[**n**,2] ⇒ **n** = 0 ∨ **n** = 1 ∨ **n** = 2 ,! 8 ()E: 7) ¡

n = 0 ∨ **n** = 1 ∨ **n** = 2 ,! 9 (⇒E: 6,8) ¡

(**n**|2 & ¬ 2 = 0 ⇒ ¬ **n** = 0) ,! 10 (∀E: P13) ¡

n|2 & ¬ 2 = 0 ⇒ ¬ **n** = 0 ,! 11 ()E: 10) ¡

¬ **n** = 0 ,! 12 (⇒E: 3,11) ¡

(**n** = 0 ∨ **n** = 1 ∨ **n** = 2) ,! 13 ()I: 9) ¡

(**n** = 0 ∨ **n** = 1 ∨ **n** = 2) & ¬ **n** = 0 ,! 14 (&I: 12,13) ¡

((**n** = 0 ∨ **n** = 1 ∨ **n** = 2) & ¬ **n** = 0 ⇒ **n** = 1 ∨ **n** = 2)
,! 15 (∀E: I3.9) ¡

(**n** = 0 ∨ **n** = 1 ∨ **n** = 2) & ¬ **n** = 0 ⇒ **n** = 1 ∨ **n** = 2
,! 16 ()E: 15) ¡

n = 1 ∨ **n** = 2 ,! 17 (⇒E: 14,16) ¡

n|2 ⇒ **n** = 1 ∨ **n** = 2 ,! 18 (⇒I: 2,17) ¡

(**n**|2 ⇒ **n** = 1 ∨ **n** = 2) ,! 19 ()I: 18) ¡

∀n (n|2 ⇒ n = 1 ∨ n = 2) ! 20 (∀I: 1,19) ¡

```
!
! 49.                                                              ¡
⊢ ∀n ( n|2 ⇔ n = 1 ∨ n = 2 )                                       ¡
  n                                          ,! 1 (Prem)          ¡
  ( n|2 ⇒ n = 1 ∨ n = 2 )                    ,! 2 (∀E: P48)       ¡
  n|2 ⇒ n = 1 ∨ n = 2                        ,! 3 (()E: 2)        ¡
    n = 1 ∨ n = 2                            ,! 4 (Prem)          ¡
      n = 1                                  ,! 5 (Prem)          ¡
      n|2                                    ,! 6 (=E: P20,5)     ¡
    n = 1 ⇒ n|2                              ,! 7 (⇒I: 5,6)       ¡
      n = 2                                  ,! 8 (Prem)          ¡
      n|2                                    ,! 9 (=E: P21,8)     ¡
    n = 2 ⇒ n|2                              ,! 10 (⇒I: 8,9)      ¡
    n|2                                      ,! 11 (∨E: 4,7,10)   ¡
  n = 1 ∨ n = 2 ⇒ n|2                        ,! 12 (⇒I: 4,11)     ¡
  n|2 ⇔ n = 1 ∨ n = 2                        ,! 13 (⇔I: 3,12)     ¡
  ( n|2 ⇔ n = 1 ∨ n = 2 )                    ,! 14 (()I: 13)      ¡
∀n ( n|2 ⇔ n = 1 ∨ n = 2 )                    ! 15 (∀I: 1,14)      ¡
!
! 50.                                                              ¡
⊢ ∀n∀m ( n|m & <[m,n] ⇒ m = 0 )                                    ¡
  n,m                                        ,! 1 (Prem)          ¡
    n|m & <[m,n]                             ,! 2 (Prem)          ¡
    n|m                                      ,! 3 (&E: 2)         ¡
    <[m,n]                                   ,! 4 (&E: 2)         ¡
      ¬ m = 0                                ,! 5 (Prem)          ¡
      n|m & ¬ m = 0                          ,! 6 (&I: 3,5)       ¡
      ( n|m & ¬ m = 0 ⇒ ≤[n,m] )              ,! 7 (∀E: P47)       ¡
      n|m & ¬ m = 0 ⇒ ≤[n,m]                  ,! 8 (()E: 7)        ¡
```

```
    ≤[n,m]                                  ,! 9 (⇒E: 6,8)      ¡
    <[m,n] & ≤[n,m]                         ,! 10 (&I: 4,9)     ¡
    ( <[m,n] & ≤[n,m] ⇒ ℱ )                 ,! 11 (∀E: V4.19)   ¡
    <[m,n] & ≤[n,m] ⇒ ℱ                     ,! 12 (()E: 11)     ¡
    ℱ                                       ,! 13 (⇒E: 10,12)   ¡
  ¬ m = 0 ⇒ ℱ                               ,! 14 (⇒I: 5,13)    ¡
  ¬¬ m = 0                                  ,! 15 (¬I: 5)       ¡
  m = 0                                     ,! 16 (¬E: 15)      ¡
n|m & <[m,n] ⇒ m = 0                        ,! 17 (⇒I: 2,16)    ¡
( n|m & <[m,n] ⇒ m = 0 )                    ,! 18 (()I: 17)     ¡
∀n∀m ( n|m & <[m,n] ⇒ m = 0 )                ! 19 (∀I: 1,18)    ¡
□

! P51-P56 relate division of the the Division Algorithm term and a
0 remainder.                                                      ¡
! 51.                                                            ¡
⊢ ∀n∀m∀q∀r ( n = ((q x m) + r) & r = 0 ⇒ m|n )                    ¡
  n,m,q,r                                   ,! 1 (Prem)         ¡
    n = ((q x m) + r) & r = 0                ,! 2 (Prem)         ¡
    n = ((q x m) + r)                        ,! 3 (&E: 2)        ¡
    r = 0                                    ,! 4 (&E: 2)        ¡
    n = ((q x m) + 0)                        ,! 5 (=E: 3,4)      ¡
    ω[(q x m)] & ω[0]                        ,! 6 (𝕋E: V1.7,5)   ¡
    ω[(q x m)]                               ,! 7 (&E: 6)        ¡
    ω[q] & ω[m]                              ,! 8 (𝕋E: V7.9,7)   ¡
    ( n = ((q x m) + 0) ⇒ n = (q x m) )      ,! 9 (∀E: V2.35;
                                             (q x m): V7.9,8)    ¡
    n = ((q x m) + 0) ⇒ n = (q x m)          ,! 10 (()E: 9)      ¡
    n = (q x m)                              ,! 11 (⇒E: 5,10)    ¡
    ( n = (q x m) ⇒ m|n )                    ,! 12 (∀E: P7)      ¡
    n = (q x m) ⇒ m|n                        ,! 13 (()E: 12)     ¡
```

m|**n** ,! 14 (⇒E: 11,13) ¡

n = ((**q** x **m**) + **r**) & **r** = 0 ⇒ **m**|**n** ,! 15 (⇒I: 2,14) ¡

(**n** = ((**q** x **m**) + **r**) & **r** = 0 ⇒ **m**|**n**) ,! 16 ()I: 15) ¡

∀n∀m∀q∀r (n = ((q x m) + r) & r = 0 ⇒ m|n)
! 17 (∀I: 1,16) ¡

□

! **52.** ¡

⊢ ∀n∀m∀q∀r (n = ((q x m) - r) & r = 0 ⇒ m|n) ¡

n,**m**,**q**,**r** ,! 1 (Prem) ¡

n = ((**q** x **m**) - **r**) & **r** = 0 ,! 2 (Prem) ¡

n = ((**q** x **m**) - **r**) ,! 3 (&E: 2) ¡

r = 0 ,! 4 (&E: 2) ¡

n = ((**q** x **m**) - 0) ,! 5 (=E: 3,4) ¡

≤[0,(**q** x **m**)] ,! 6 (𝕋E: V5.7,5) ¡

ω[**q**] & ω[**m**] ,! 7 (𝕋E: V7.9,6) ¡

(**n** = ((**q** x **m**) - 0) ⇒ **n** = (**q** x **m**)) ,! 8 (∀E: V6.30;
(**q** x **m**): V7.9,7) ¡

n = ((**q** x **m**) - 0) ⇒ **n** = (**q** x **m**) ,! 9 ()E: 8) ¡

n = (**q** x **m**) ,! 10 (⇒E: 5,9) ¡

(**n** = (**q** x **m**) ⇒ **m**|**n**) ,! 12 (∀E: P7) ¡

n = (**q** x **m**) ⇒ **m**|**n** ,! 13 ()E: 12) ¡

m|**n** ,! 14 (⇒E: 10,13) ¡

n = ((**q** x **m**) - **r**) & **r** = 0 ⇒ **m**|**n** ,! 15 (⇒I: 2,14) ¡

(**n** = ((**q** x **m**) - **r**) & **r** = 0 ⇒ **m**|**n**) ,! 16 ()I: 15) ¡

∀n∀m∀q∀r (n = ((q x m) - r) & r = 0 ⇒ m|n)
! 17 (∀I: 1,16) ¡

□

! **53.** ¡

⊢ ∀n∀m∀q∀r (n = ((q x m) + r) & ¬ m|n ⇒ ¬ r = 0) ¡

n,**m**,**q**,**r** ,! 1 (Prem) ¡

n = ((**q** x **m**) + **r**) & ¬ **m**|**n** ,! 2 (Prem) ¡

n = ((**q** x **m**) + **r**) ,! 3 (&E: 2) ¡

¬ **m**|**n** ,! 4 (&E: 2) ¡

r = 0 ,! 5 (Prem) ¡

n = ((**q** x **m**) + **r**) & **r** = 0 ,! 6 (&I: 3,5) ¡

(**n** = ((**q** x **m**) + **r**) & **r** = 0 ⇒ **m**|**n**)
,! 7 (∀E: P51) ¡

n = ((**q** x **m**) + **r**) & **r** = 0 ⇒ **m**|**n** ,! 8 ()E: 7) ¡

m|**n** ,! 9 (⇒E: 6,8) ¡

ℱ ,! 10 (ℱI: 4,9) ¡

r = 0 ⇒ ℱ ,! 11 (⇒I: 5,10) ¡

¬ **r** = 0 ,! 12 (¬I: 11) ¡

n = ((**q** x **m**) + **r**) & ¬ **m**|**n** ⇒ ¬ **r** = 0 ,! 13 (⇒I: 2,12) ¡

(**n** = ((**q** x **m**) + **r**) & ¬ **m**|**n** ⇒ ¬ **r** = 0)
,! 14 ()I: 13) ¡

∀n∀m∀q∀r (n = ((q x m) + r) & ¬ m|n ⇒ ¬ r = 0)
! 15 (∀I: 1,14) ¡

□

! **54.** ¡

⊢ ∀n∀m∀q∀r (n = ((q x m) - r) & ¬ m|n ⇒ ¬ r = 0) ¡

n,**m**,**q**,**r** ,! 1 (Prem) ¡

n = ((**q** x **m**) - **r**) & ¬ **m**|**n** ,! 2 (Prem) ¡

n = ((**q** x **m**) - **r**) ,! 3 (&E: 2) ¡

¬ **m**|**n** ,! 4 (&E: 2) ¡

r = 0 ,! 5 (Prem) ¡

n = ((**q** x **m**) - **r**) & **r** = 0 ,! 6 (&I: 3,5) ¡

(**n** = ((**q** x **m**) - **r**) & **r** = 0 ⇒ **m**|**n**)
,! 7 (∀E: P52) ¡

n = ((**q** x **m**) - **r**) & **r** = 0 ⇒ **m**|**n** ,! 8 ()E: 7) ¡

m|**n** ,! 9 (⇒E: 6,8) ¡

```
    𝔉                                   ,! 10 (𝔉I: 4,9)    ¡
  r = 0 ⇒ 𝔉                             ,! 11 (⇒I: 5,10)   ¡
  ¬ r = 0                               ,! 12 (¬I: 11)     ¡
n = ((q x m) - r) & ¬ m|n ⇒ ¬ r = 0      ,! 13 (⇒I: 2,12)   ¡
( n = ((q x m) - r) & ¬ m|n ⇒ ¬ r = 0 )
                                        ,! 14 ()I: 13)     ¡
∀n∀m∀q∀r ( n = ((q x m) - r) & ¬ m|n ⇒ ¬ r = 0 )
                                         ! 15 (∀I: 1,14)   ¡
□
! 55.                                                      ¡
⊢ ∀n∀m∀q∀r ( n = ((q x m) + r) & <[r,m] & m|n ⇒ r = 0 )     ¡
  n,m,q,r                               ,! 1 (Prem)        ¡
    n = ((q x m) + r) & <[r,m] & m|n    ,! 2 (Prem)        ¡
    n = ((q x m) + r)                   ,! 3 (&E: 2)       ¡
    <[r,m]                              ,! 4 (&E: 2)       ¡
    m|n                                 ,! 5 (&E: 2)       ¡
    n = ((q x m) + r) & m|n             ,! 6 (&I: 3,5)     ¡
    ω[(q x m)] & ω[r]                   ,! 7 (𝕋E: V1.7,3)  ¡
    ω[(q x m)]                          ,! 8 (&E: 7)       ¡
    ω[q] & ω[m]                         ,! 9 (𝕋E: V7.9,8)  ¡
    ω[q]                                ,! 10 (&E: 9)      ¡
    ω[m]                                ,! 11 (&E: 9)      ¡
    ω[m] & ω[q]                         ,! 12 (&I: 10,11)  ¡
    ( ω[m] & ω[q] ⇒ m|(q x m) )          ,! 13 (∀E: P9)     ¡
    ω[m] & ω[q] ⇒ m|(q x m)              ,! 14 ()E: 13)     ¡
    m|(q x m)                           ,! 15 (⇒E: 12,14)  ¡
    n = ((q x m) + r) & m|n & m|(q x m) ,! 16 (&I: 6,15)    ¡
    ( n = ((q x m) + r) & m|n & m|(q x m) ⇒ m|r )
                                        ,! 17 (∀E: P36;
                                        (q x m): V7.9,9)   ¡
```

n = ((**q** x **m**) + **r**) & **m**|**n** & **m**|(**q** x **m**) ⇒ **m**|**r**
,! 18 (()E: 17) ¡

m|**r** ,! 19 (⇒E: 16,18) ¡

m|**r** & <[**r**,**m**] ,! 20 (&I: 4,19) ¡

(**m**|**r** & <[**r**,**m**] ⇒ **r** = 0) ,! 21 (∀E: P50) ¡

m|**r** & <[**r**,**m**] ⇒ **r** = 0 ,! 22 (()E: 21) ¡

r = 0 ,! 23 (⇒E: 20,22) ¡

n = ((**q** x **m**) + **r**) & <[**r**,**m**] & **m**|**n** ⇒ **r** = 0
,! 24 (⇒I: 2,23) ¡

(**n** = ((**q** x **m**) + **r**) & <[**r**,**m**] & **m**|**n** ⇒ **r** = 0)
,! 25 (()I: 24) ¡

∀n∀m∀q∀r (n = ((q x m) + r) & <[r,m] & m|n ⇒ r = 0)
! 26 (∀I: 1,25) ¡

□

! **56.** For every finite set of finite numbers, there exists a non-zero number which they all divide. P56 is used to establish P57, which in turn is used by the proof of Euclid's theorem that there are an infinity of prime numbers. ¡

⊢ ∀P (*f* P & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x))) ¡

! We first prove
∀n (ω[n]
⇒ ∀P (ℕ[n,P] & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)))
taking ϕ to be
∀P (ℕ[n,P] & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)))
It must be shown that
∀P (ℕ[0,P] & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)))
and
∀n∀m (ω[n] & σ[n,m]
& ∀P (ℕ[n,P] & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)))
⇒ ∀P (ℕ[m,P] & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)))) ¡

! To prove:
∀P (ℕ[0,P] & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x))) ¡

```
  P                                          ,! 1 (Prem)          ¡
    ℕ[0,P] & P ⊆ ω & ¬ P[0]                  ,! 2 (Prem)          ¡
    ℕ[0,P]                                   ,! 3 (&E)            ¡
    ω[1] & ¬ 1 = 0                           ,! 4 (&I: IV9.2,IV9.6)
                                                                  ¡
    ( ℕ[0,P] ⇒ ¬ ∃x P[x] )                   ,! 5 (∀E: IV3.5)     ¡
    ℕ[0,P] ⇒ ¬ ∃x P[x]                      ,! 6 (()E: 5)        ¡
    ¬ ∃x P[x]                                ,! 7 (⇒E: 3,6)       ¡
      y                                      ,! 8 (Prem)          ¡
        P[y]                                 ,! 9 (Prem)          ¡
        ∃x P[x]                              ,! 10 (∃I: 9)        ¡
          ¬ y|1                              ,! 11 (Prem)         ¡
          ℱ                                  ,! 12 (ℱI: 7,9)      ¡
        ¬ y|1 ⇒ ℱ                            ,! 13 (⇒I: 11,12)    ¡
        ¬¬ y|1                               ,! 14 (¬I: 13)       ¡
        y|1                                  ,! 15 (¬E: 14)       ¡
      P[y] ⇒ y|1                             ,! 16 (⇒I: 9,15)     ¡
      (P[y] ⇒ y|1)                           ,! 17 (()I: 16)      ¡
    ∀y (P[y] ⇒ y|1)                          ,! 18 (∀I: 17)       ¡
    ω[1] & ¬ 1 = 0 & ∀y (P[y] ⇒ y|1)          ,! 19 (&I: 4,18)     ¡
    (ω[1] & ¬ 1 = 0 & ∀y (P[y] ⇒ y|1))        ,! 20 (()I: 19)      ¡
    ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x))
                                             ,! 21 (∃I: 20)       ¡
  ℕ[0,P] & P ⊆ ω & ¬ P[0]
  ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x))
                                             ,! 22 (⇒I: 2,21)     ¡
  ( ℕ[0,P] & P ⊆ ω & ¬ P[0]
    ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
                                             ,! 23 (()I: 22)      ¡
∀P ( ℕ[0,P] & P ⊆ ω & ¬ P[0]
     ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
```

```
                                                ,! 24 (∀I: 1,23)    ¡

!  To prove:
     ∀n∀m ( ω[n] & σ[n,m]
            & ∀P ( ℕ[n,P] & P ⊆ ω & ¬ P[0]
                   ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
            ⇒ ∀P ( ℕ[m,P] & P ⊆ ω & ¬ P[0]
                   ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) ) )
                                                                    ¡

  n,m                                           ,! 25 (Prem)        ¡

    ω[n] & σ[n,m]
    & ∀P ( ℕ[n,P] & P ⊆ ω & ¬ P[0]
           ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
                                                ,! 26 (Prem)        ¡

    ω[n] & σ[n,m]                               ,! 27 (&E: 26)      ¡

    ∀P ( ℕ[n,P] & P ⊆ ω & ¬ P[0]
         ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
                                                ,! 28 (&E: 26)      ¡

    ( ω[n] & σ[n,m] ⇒ (n') = m )                ,! 29 (∀E: IV8.18)  ¡

    ω[n] & σ[n,m] ⇒ (n') = m                    ,! 30 ()E: 29)      ¡

    (n') = m                                    ,! 31 (⇒E: 27,30)   ¡

    ¬ (n') = 0                                  ,! 32 (∀E: IV8.32)  ¡

    ¬ m = 0                                     ,! 33 (=E: 31,32)   ¡

      P                                         ,! 34 (Prem)        ¡

        ℕ[m,P] & P ⊆ ω & ¬ P[0]                 ,! 35 (Prem)        ¡

        ℕ[m,P]                                  ,! 36 (&E: 35)      ¡

        P ⊆ ω                                   ,! 37 (&E: 35)      ¡

        ¬ P[0]                                  ,! 38 (&E: 35)      ¡

        ℕ[m,P] & ¬ m = 0                        ,! 39 (&I: 33,36)   ¡

        ( ℕ[m,P] & ¬ m = 0 ⇒ ∃x P[x] )          ,! 40 (∀E: IV3.17)  ¡

        ℕ[m,P] & ¬ m = 0 ⇒ ∃x P[x]              ,! 41 ()E: 40)      ¡

        ∃x P[x]                                 ,! 42 (⇒E: 39,41)   ¡

        P[a]                                    ,! 43 (∃E: 42)      ¡

        ω[n] & σ[n,m] & P[a]                    ,! 44 (&I: 27,43)   ¡
```

$\omega[\mathbf{n}] \;\&\; \sigma[\mathbf{n},\mathbf{m}] \;\&\; \mathbf{P}[\mathbf{a}] \;\&\; \mathbb{N}[\mathbf{m},\mathbf{P}]$,! 45 (&I: 36,44) ¡

$(\omega[\mathbf{n}] \;\&\; \sigma[\mathbf{n},\mathbf{m}] \;\&\; \mathbf{P}[\mathbf{a}] \;\&\; \mathbb{N}[\mathbf{m},\mathbf{P}] \Rightarrow \mathbb{N}[\mathbf{n},(\mathbf{P} \setminus (\mathbf{a}^\bullet))])$,! 46 (∀E: IV2.11) ¡

$\omega[\mathbf{n}] \;\&\; \sigma[\mathbf{n},\mathbf{m}] \;\&\; \mathbf{P}[\mathbf{a}] \;\&\; \mathbb{N}[\mathbf{m},\mathbf{P}] \Rightarrow \mathbb{N}[\mathbf{n},(\mathbf{P} \setminus (\mathbf{a}^\bullet))]$,! 47 (()E: 46) ¡

$\mathbb{N}[\mathbf{n},(\mathbf{P} \setminus (\mathbf{a}^\bullet))]$,! 48 (⇒E: 45,47) ¡

$(\mathbf{P} \subseteq \omega \Rightarrow (\mathbf{P} \setminus (\mathbf{a}^\bullet)) \subseteq \omega)$,! 49 (∀E: II7.15) ¡

$\mathbf{P} \subseteq \omega \Rightarrow (\mathbf{P} \setminus (\mathbf{a}^\bullet)) \subseteq \omega$,! 50 (()E: 49) ¡

$(\mathbf{P} \setminus (\mathbf{a}^\bullet)) \subseteq \omega$,! 51 (⇒E: 37,50) ¡

$\mathbb{N}[\mathbf{n},(\mathbf{P} \setminus (\mathbf{a}^\bullet))] \;\&\; (\mathbf{P} \setminus (\mathbf{a}^\bullet)) \subseteq \omega$,! 52 (&I: 48,51) ¡

$(\neg \mathbf{P}[0] \Rightarrow \neg (\mathbf{P} \setminus (\mathbf{a}^\bullet))[0])$,! 53 (∀E: II7.7) ¡

$\neg \mathbf{P}[0] \Rightarrow \neg (\mathbf{P} \setminus (\mathbf{a}^\bullet))[0]$,! 54 (()E: 53) ¡

$\neg (\mathbf{P} \setminus (\mathbf{a}^\bullet))[0]$,! 55 (⇒E: 38,54) ¡

$\mathbb{N}[\mathbf{n},(\mathbf{P} \setminus (\mathbf{a}^\bullet))] \;\&\; (\mathbf{P} \setminus (\mathbf{a}^\bullet)) \subseteq \omega \;\&\; \neg (\mathbf{P} \setminus (\mathbf{a}^\bullet))[0]$,! 56 (&I: 52,55) ¡

! Applying the induction hypothesis... ¡

$(\mathbb{N}[\mathbf{n},(\mathbf{P} \setminus (\mathbf{a}^\bullet))] \;\&\; (\mathbf{P} \setminus (\mathbf{a}^\bullet)) \subseteq \omega \;\&\; \neg (\mathbf{P} \setminus (\mathbf{a}^\bullet))[0] \Rightarrow \exists x\, (\omega[x] \;\&\; \neg\, x = 0 \;\&\; \forall y\, ((\mathbf{P} \setminus (\mathbf{a}^\bullet))[y] \Rightarrow y|x)))$,! 57 (∀E: 28) ¡

$\mathbb{N}[\mathbf{n},(\mathbf{P} \setminus (\mathbf{a}^\bullet))] \;\&\; (\mathbf{P} \setminus (\mathbf{a}^\bullet)) \subseteq \omega \;\&\; \neg (\mathbf{P} \setminus (\mathbf{a}^\bullet))[0] \Rightarrow \exists x\, (\omega[x] \;\&\; \neg\, x = 0 \;\&\; \forall y\, ((\mathbf{P} \setminus (\mathbf{a}^\bullet))[y] \Rightarrow y|x))$,! 58 (()E: 57) ¡

$\exists x\, (\omega[x] \;\&\; \neg\, x = 0 \;\&\; \forall y\, ((\mathbf{P} \setminus (\mathbf{a}^\bullet))[y] \Rightarrow y|x\,))$,! 59 (⇒E: 56,58) ¡

$(\omega[\mathbf{x}] \;\&\; \neg\, \mathbf{x} = 0 \;\&\; \forall y\, ((\mathbf{P} \setminus (\mathbf{a}^\bullet))[y] \Rightarrow y|\mathbf{x}))$,! 60 (∃E: 59) ¡

$\omega[\mathbf{x}] \;\&\; \neg\, \mathbf{x} = 0 \;\&\; \forall y\, ((\mathbf{P} \setminus (\mathbf{a}^\bullet))[y] \Rightarrow y|\mathbf{x})$,! 61 (()E: 60) ¡

$\omega[\mathbf{x}]$,! 62 (&E: 61) ¡

$\neg\, \mathbf{x} = 0$,! 63 (&E: 61) ¡

$\forall y\, ((\mathbf{P} \setminus (\mathbf{a}^\bullet))[y] \Rightarrow y|\mathbf{x})$,! 64 (&E: 61) ¡

$\mathbf{P}[\mathbf{a}] \;\&\; \mathbf{P} \subseteq \omega$,! 65 (&I: 37,43) ¡

(**P**[**a**] & **P** ⊆ ω ⇒ ω[**a**]) ,! 66 (∀E: II1.2) ¡

P[**a**] & **P** ⊆ ω ⇒ ω[**a**] ,! 67 (()E: 66) ¡

ω[**a**] ,! 68 (⇒E: 65,67) ¡

ω[**a**] & ω[**x**] ,! 69 (&I: 62,68) ¡

(ω[**a**] & ω[**x**] ⇒ ω[(**a** x **x**)]) ,! 70 (∀E: V7.10) ¡

ω[**a**] & ω[**x**] ⇒ ω[(**a** x **x**)] ,! 71 (()E: 70) ¡

ω[(**a** x **x**)] ,! 72 (⇒E: 69,71) ¡

a = 0 ,! 73 (Prem) ¡

P[0] ,! 74 (=E: 43,73) ¡

ℱ ,! 75 (ℱI: 38,74) ¡

a = 0 ⇒ ℱ ,! 76 (⇒I: 73,75) ¡

¬ **a** = 0 ,! 77 (¬I: 76) ¡

¬ **a** = 0 & ¬ **x** = 0 ,! 78 (&I: 63,77) ¡

(¬ **a** = 0 & ¬ **x** = 0 ⇒ ¬ (**a** x **x**) = 0)
,! 79 (∀E: V8.40) ¡

¬ **a** = 0 & ¬ **x** = 0 ⇒ ¬ (**a** x **x**) = 0
,! 80 (()E: 79) ¡

¬ (**a** x **x**) = 0 ,! 81 (⇒E: 78,80) ¡

ω[(**a** x **x**)] & ¬ (**a** x **x**) = 0 ,! 82 (&I: 72,81) ¡

y ,! 83 (Prem) ¡

P[**y**] ,! 84 (Prem) ¡

(**P**[**y**] ⇒ (**P** \ (**a**•))[**y**] ∨ (**a**•)[**y**])
,! 85 (∀E: II7.10) ¡

P[**y**] ⇒ (**P** \ (**a**•))[**y**] ∨ (**a**•)[**y**]
,! 86 (()E: 85) ¡

(**P** \ (**a**•))[**y**] ∨ (**a**•)[**y**] ,! 87 (⇒E: 84,86) ¡

(**P** \ (**a**•))[**y**] ,! 88 (Prem) ¡

((**P** \ (**a**•))[**y**] ⇒ **y**|**x**) ,! 89 (∀E: 64) ¡

(**P** \ (**a**•))[**y**] ⇒ **y**|**x** ,! 90 (()E: 89) ¡

y|**x** ,! 91 (⇒E: 88,90) ¡

$\mathbf{y}|\mathbf{x}$ & $\omega[\mathbf{a}]$,! 92 (&I: 68,91) ¡

($\mathbf{y}|\mathbf{x}$ & $\omega[\mathbf{a}]$ ⇒ $\mathbf{y}|(\mathbf{a}$ x $\mathbf{x})$) ,! 93 (∀E: P28) ¡

$\mathbf{y}|\mathbf{x}$ & $\omega[\mathbf{a}]$ ⇒ $\mathbf{y}|(\mathbf{a}$ x $\mathbf{x})$,! 94 (()E: 93) ¡

$\mathbf{y}|(\mathbf{a}$ x $\mathbf{x})$,! 95 (⇒E: 92,94) ¡

$(\mathbf{P} \setminus (\mathbf{a}^{\bullet}))[\mathbf{y}]$ ⇒ $\mathbf{y}|(\mathbf{a}$ x $\mathbf{x})$,! 96 (⇒I: 88,95) ¡

$(\mathbf{a}^{\bullet})[\mathbf{y}]$,! 97 (Prem) ¡

($\omega[\mathbf{a}]$ & $\omega[\mathbf{x}]$ ⇒ $\mathbf{a}|(\mathbf{a}$ x $\mathbf{x})$)
,! 98 (∀E: P8) ¡

$\omega[\mathbf{a}]$ & $\omega[\mathbf{x}]$ ⇒ $\mathbf{a}|(\mathbf{a}$ x $\mathbf{x})$,! 99 (()E: 98) ¡

$\mathbf{a}|(\mathbf{a}$ x $\mathbf{x})$,! 100 (⇒E: 69,99) ¡

($(\mathbf{a}^{\bullet})[\mathbf{y}]$ ⇒ $\mathbf{y} = \mathbf{a}$) ,! 101 (∀E: II8.3) ¡

$(\mathbf{a}^{\bullet})[\mathbf{y}]$ ⇒ $\mathbf{y} = \mathbf{a}$,! 102 (()E: 101) ¡

$\mathbf{y} = \mathbf{a}$,! 103 (⇒E: 97,102)
¡

$\mathbf{y}|(\mathbf{a}$ x $\mathbf{x})$,! 104 (=E: 100,103)
¡

$(\mathbf{a}^{\bullet})[\mathbf{y}]$ ⇒ $\mathbf{y}|(\mathbf{a}$ x $\mathbf{x})$,! 105 (⇒I: 97,104)
¡

$\mathbf{y}|(\mathbf{a}$ x $\mathbf{x})$,! 106 (∨E: 87,96,105)
¡

$\mathbf{P}[\mathbf{y}]$ ⇒ $\mathbf{y}|(\mathbf{a}$ x $\mathbf{x})$,! 107 (⇒I: 84,106)
¡

$(\mathbf{P}[\mathbf{y}]$ ⇒ $\mathbf{y}|(\mathbf{a}$ x $\mathbf{x}))$,! 108 (()I: 107) ¡

∀y ($\mathbf{P}$[y] ⇒ y|($\mathbf{a}$ x $\mathbf{x}$)) ,! 109 (∀I: 108) ¡

$\omega[(\mathbf{a}$ x $\mathbf{x})]$ & ¬ ($\mathbf{a}$ x $\mathbf{x}$) = 0 & ∀y ($\mathbf{P}$[y] ⇒ y|($\mathbf{a}$ x $\mathbf{x}$))
,! 110 (&I: 82,109) ¡

($\omega[(\mathbf{a}$ x $\mathbf{x})]$ & ¬ ($\mathbf{a}$ x $\mathbf{x}$) = 0 & ∀y ($\mathbf{P}$[y] ⇒ y|($\mathbf{a}$ x $\mathbf{x}$)))
,! 111 (()I: 110) ¡

∃x (ω[x] & ¬ x = 0 & ∀y ($\mathbf{P}$[y] ⇒ y|x))
,! 112 (∃I: 111;
($\mathbf{a}$ x $\mathbf{x}$): V7.9,69) ¡

$\mathbb{N}[\mathbf{m},\mathbf{P}]$ & $\mathbf{P} \subseteq \omega$ & ¬ $\mathbf{P}[0]$

```
      ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x))
                                          ,! 113 (⇒I: 35,112)
                                                              ¡

      ( ℕ[m,P] & P ⊆ ω & ¬ P[0]
        ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
                                          ,! 114 (()I: 113)   ¡

    ∀P ( ℕ[m,P] & P ⊆ ω & ¬ P[0]
         ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
                                          ,! 115 (∀I: 34,114) ¡

  ω[n] & σ[n,m]
  & ∀P ( ℕ[n,P] & P ⊆ ω & ¬ P[0]
         ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
  ⇒ ∀P ( ℕ[m,P] & P ⊆ ω & ¬ P[0]
         ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
                                          ,! 116 (⇒I: 26,115)
                                                              ¡

  ( ω[n] & σ[n,m]
    & ∀P ( ℕ[n,P] & P ⊆ ω & ¬ P[0]
           ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
    ⇒ ∀P ( ℕ[m,P] & P ⊆ ω & ¬ P[0]
           ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) ) )
                                          ,! 117 (()I: 116)   ¡


∀n∀m ( ω[n] & σ[n,m]
       & ∀P ( ℕ[n,P] & P ⊆ ω & ¬ P[0]
              ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) )
       ⇒ ∀P ( ℕ[m,P] & P ⊆ ω & ¬ P[0]
              ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) ) )
                                          ,! 118 (∀I: 25,117) ¡

∀n ( ω[n]
     ⇒ ∀P ( ℕ[n,P] & P ⊆ ω & ¬ P[0]
            ⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)) ) )
                                           ! 119 (Induct: 24,118)
                                                              ¡

! Now to prove the proposition proper...                      ¡

  P                                       ,! 120 (Prem)       ¡

    ƒ P & P ⊆ ω & ¬ P[0]                   ,! 121 (Prem)       ¡

    ƒ P                                   ,! 122 (&E: 121)    ¡

    P ⊆ ω & ¬ P[0]                        ,! 123 (&E: 121)    ¡

    ∃n ( ω[n] & ℕ[n,P] )                  ,! 124 (𝕊E: IV5.1,122)
                                                              ¡
```

(ω[**n**] & ℕ[**n**,**P**]) ,! 125 (∃E: 124) ¡

ω[**n**] & ℕ[**n**,**P**] ,! 126 ()E: 125) ¡

ω[**n**] ,! 127 (&E: 126) ¡

ℕ[**n**,**P**] ,! 128 (&E: 126) ¡

(ω[**n**]
⇒ ∀P (ℕ[**n**,P] & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x))))
,! 129 (∀E: 119) ¡

ω[**n**]
⇒ ∀P (ℕ[**n**,P] & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)))
,! 130 ()E: 129) ¡

∀P (ℕ[**n**,P] & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)))
,! 131 (⇒E: 127,130)
¡

ℕ[**n**,**P**] & **P** ⊆ ω & ¬ **P**[0] ,! 132 (&I: 123,128)
¡

(ℕ[**n**,**P**] & **P** ⊆ ω & ¬ **P**[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (**P**[y] ⇒ y|x)))
,! 133 (∀E: 131) ¡

ℕ[**n**,**P**] & **P** ⊆ ω & ¬ **P**[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (**P**[y] ⇒ y|x))
,! 134 ()E: 133) ¡

∃x (ω[x] & ¬ x = 0 & ∀y (**P**[y] ⇒ y|x))
,! 135 (⇒E: 132,134)
¡

f **P** & **P** ⊆ ω & ¬ **P**[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (**P**[y] ⇒ y|x))
,! 136 (⇒I: 121,135)
¡

(*f* **P** & **P** ⊆ ω & ¬ **P**[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (**P**[y] ⇒ y|x)))
,! 137 ()I: 136) ¡

∀P (*f* P & P ⊆ ω & ¬ P[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (P[y] ⇒ y|x)))
! 138 (∀I: 120,137)
¡

□

! **57.** P57's premise can be weakened, but the actual one makes the proof easier, and does not disturb our sole use of the proposition, to prove Euclid's theorem that the prime numbers are infinite. ¡

⊢ ∀P (*f* P & P ⊆ ω & ¬ P[0] & ¬ P[1]
⇒ ∃x (ω[x] & ¬ x = 1 & ∀y (P[y] ⇒ ¬ y|x))) ¡

P ,! 1 (Prem) ¡

f **P** & **P** ⊆ ω & ¬ **P**[0] & ¬ **P**[1] ,! 2 (Prem) ¡

f **P** & **P** ⊆ ω & ¬ **P**[0] ,! 3 (&E: 2) ¡

¬ **P**[1] ,! 4 (&E: 2) ¡

(*f* **P** & **P** ⊆ ω & ¬ **P**[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (**P**[y] ⇒ y|x)))
,! 5 (∀E: P56) ¡

f **P** & **P** ⊆ ω & ¬**P**[0]
⇒ ∃x (ω[x] & ¬ x = 0 & ∀y (**P**[y] ⇒ y|x))
,! 6 (()E: 5) ¡

∃x (ω[x] & ¬ x = 0 & ∀y (**P**[y] ⇒ y|x))
,! 7 (⇒E: 3,6) ¡

(ω[**x**] & ¬ **x** = 0 & ∀y (**P**[y] ⇒ y|**x**)) ,! 8 (∃E: 7) ¡

ω[**x**] & ¬ **x** = 0 & ∀y (**P**[y] ⇒ y|**x**) ,! 9 (()E: 8) ¡

ω[**x**] ,! 10 (&E: 9) ¡

¬ **x** = 0 ,! 11 (&E: 9) ¡

∀y (**P**[y] ⇒ y|**x**) ,! 12 (&E: 9) ¡

ω[**x**] & ω[1] ,! 13 (&I: IV9.2,10)
¡

(ω[**x**] & ω[1] ⇒ ω[(**x**+1)]) ,! 14 (∀E: V1.8) ¡

ω[**x**] & ω[1] ⇒ ω[(**x**+1)] ,! 15 (()E: 14) ¡

ω[(**x**+1)] ,! 16 (⇒E: 13,15) ¡

(**x**+1) = 1 ,! 17 (Prem) ¡

((**x**+1) = 1 ⇒ **x** = 0) ,! 18 (∀E: V2.39) ¡

(**x**+1) = 1 ⇒ **x** = 0 ,! 19 (()E: 18) ¡

x = 0 ,! 20 (⇒E: 17,19) ¡

```
  ℱ                                  ,! 21 (ℱI: 11,20)  ¡

(x+1) = 1 ⇒ ℱ                        ,! 22 (⇒I: 17,21)  ¡

¬ (x+1) = 1                          ,! 23 (¬I: 22)     ¡

ω[(x+1)] & ¬ (x+1) = 1                ,! 24 (&I: 16,23)  ¡

  y                                  ,! 25 (Prem)       ¡

    P[y]                             ,! 26 (Prem)       ¡

      y|(x+1)                        ,! 27 (Prem)       ¡

      (P[y] ⇒ y|x)                   ,! 28 (∀E: 12)     ¡

      P[y] ⇒ y|x                     ,! 29 (()E: 28)    ¡

      y|x                            ,! 30 (⇒E: 26,29)  ¡

      y|(x+1) & y|x                  ,! 31 (&I: 27,30)  ¡

      ( y|(x+1) & y|x ⇒ y|1 )        ,! 32 (∀E: P31)    ¡

      y|(x+1) & y|x ⇒ y|1            ,! 33 (()E: 32)    ¡

      y|1                            ,! 34 (⇒E: 31,33)  ¡

      ( y|1 ⇒ y = 1 )                ,! 35 (∀E: P15)    ¡

      y|1 ⇒ y = 1                    ,! 36 (()E: 35)    ¡

      y = 1                          ,! 37 (⇒E: 34,36)  ¡

      P[1]                           ,! 38 (=E: 26,37)  ¡

      ℱ                              ,! 39 (ℱI: 4,38)   ¡

    y|(x+1) ⇒ ℱ                      ,! 40 (⇒I: 27,39)  ¡

    ¬ y|(x+1)                        ,! 41 (¬I: 40)     ¡

  P[y] ⇒ ¬ y|(x+1)                   ,! 42 (⇒I: 26,41)  ¡

  (P[y] ⇒ ¬ y|(x+1))                 ,! 43 (()I: 42)    ¡

∀y (P[y] ⇒ ¬ y|(x+1))                ,! 44 (∀I: 25,43)  ¡

ω[(x+1)] & ¬ (x+1) = 1 & ∀y (P[y] ⇒ ¬ y|(x+1))
                                     ,! 45 (&I: 24,44)  ¡

(ω[(x+1)] & ¬ (x+1) = 1 & ∀y (P[y] ⇒ ¬ y|(x+1)))
                                     ,! 46 (()I: 45)    ¡

∃x (ω[x] & ¬ x = 1 & ∀y (P[y] ⇒ ¬ y|x))
                                     ,! 47 (∃I: 46;
```

V1.7,13) ¡

f **P** & **P** ⊆ ω & ¬ **P**[0] & ¬ **P**[1]
⇒ ∃x (ω[x] & ¬ x = 1 & ∀y (**P**[y] ⇒ ¬ y|x))
,! 48 (⇒I: 2,47) ¡

(*f* **P** & **P** ⊆ ω & ¬ **P**[0] & ¬ **P**[1]
⇒ ∃x (ω[x] & ¬ x = 1 & ∀y (**P**[y] ⇒ ¬ y|x)))
,! 49 (()I: 48) ¡

∀P (*f* P & P ⊆ ω & ¬ P[0] & ¬ P[1]
⇒ ∃x (ω[x] & ¬ x = 1 & ∀y (P[y] ⇒ ¬ y|x)))
! 50 (∀I: 1,49) ¡

□