```
divides_iff_rem_zero  THM

⊢  ∀a:ℤ, b:ℤ⁻⁰. b | a ⟺ (a rem b) = 0  by GenUnivCD
|
|\
| 1. a : ℤ
| 2. b : ℤ⁻⁰
| 3. b | a
| ⊢  (a rem b) = 0  by Assert (∀i:ℕ, j:ℕ⁺. j | i ⇒ (i rem j) = 0)
| |
| |\
| | .....assertion .....
| | ⊢  ∀i:ℕ, j:ℕ⁺. j | i ⇒ (i rem j) = 0
| | | by OnHyps [3;2;1] Thin THEN UnivCD
| | |
| | 1. i : ℕ
| | 2. j : ℕ⁺
| | 3. j | i
| | ⊢  (i rem j) = 0
| | | by RWH
| | |    (LemmaC
| | |     Thm* ∀a:ℤ, n:ℤ⁻⁰. (a rem n) = a-(a ÷ n)·n    {rem_to_div})
| | |    0
| | |
| | ⊢  i-(i ÷ j)·j = 0
| | | by Inst
| | |    Thm* ∀a:ℕ, n:ℕ⁺. ∃q:ℕ. Div(a;n;q) & (a ÷ n) = q    {div_elim}
| | |    [i;j]
| | |
| | 4. ∃q:ℕ. Div(i;j;q) & (i ÷ j) = q
| | ⊢  i-(i ÷ j)·j = 0
| | | by (Analyze 4 THEN Analyze 5 THEN HypSubst 6 0) THEN (Thin 6)
| | |
| | 4. q : ℕ
| | 5. Div(i;j;q)
| | ⊢  i-q·j = 0
| | | by Unfold ‘div_nrel‘ 5 THEN Analyze 5 THEN Analyze 3
| | |
| | 3. c : ℤ
| | 4. i = j·c
| | 5. q : ℕ
| | 6. j·q≤i
| | 7. i<j·(q+1)
| | ⊢  i-q·j = 0  by (OnMClauses [0;6;7] (HypSubst 4)) THEN (Thin 4)
| | |
| | 4. q : ℕ
| | 5. j·q≤j·c
| | 6. j·c<j·(q+1)
| | ⊢  j·c-q·j = 0
| | | by (FwdThru
| | |     Thm* ∀a,b:ℤ, n:ℕ⁺. n·a≤n·b ⇒ a≤b    {mul_cancel_in_le}
| | |     [5])
| | |    THEN
| | |    (FwdThru
| | |     Thm* ∀a,b:ℤ, n:ℕ⁺. n·a<n·b ⇒ a<b    {mul_cancel_in_lt}
```

```
| | |     [6])
| | |    THEN
| | |    (OnHyps [6;5] Thin)
| | |
| | 5. q≤c
| | 6. c<q+1
| | ⊢  j·c-q·j = 0
| |   by (Using [‘n’,(j·q)]
| |       (BackThru
| |        Thm* ∀a,b,n:ℤ. a = b ⟺ a+n = b+n    {add_mono_wrt_eq}))
| |      THEN
| |      (Assert (j·c = j·q))
| |
| .\
| . 4. ∀i:ℕ, j:ℕ⁺. j | i ⇒ (i rem j) = 0
| . ⊢  (a rem b) = 0  by (Decide (a≥0)) THEN (Decide (b≥0))
| . |
| . |\
| . | 5. a≥0
| . | 6. b≥0
| . | ⊢  (a rem b) = 0  by BackThru 4
| . |
| . |\
| . | 5. a≥0
| . | 6. ¬b≥0
| . | ⊢  (a rem b) = 0
| . | | by RWH
| . | |    (LemmaC
| . | |     Thm* ∀a:ℕ, n:{...-1}. (a rem n) = (a rem -n)
| . | |     {rem_4_to_1})
| . | |    0
| . | |
| . | ⊢  (a rem -b) = 0  by BackThru 4
| . | |
| . | ⊢  -b | a
| . |   by BackThru Thm* ∀a,b:ℤ. a | b ⟺ -a | b    {divides_invar_1}
| . |
| . |\
| . | 5. ¬a≥0
| . | 6. b≥0
| . | ⊢  (a rem b) = 0
| . | | by RWH
| . | |    (LemmaC
| . | |     Thm* ∀a:{...0}, n:ℕ⁺. (a rem n) = -((-a) rem n)
| . | |     {rem_2_to_1})
| . | |    0
| . | |

| . | ⊢  -((-a) rem b) = 0  by Rewrite (HigherC (HypC 4)) 0
| . | |
| . | .....rewrite subgoal .....
| . | ⊢  b | -a
| . |   by BackThru Thm* ∀a,b:ℤ. a | b ⟺ a | -b    {divides_invar_2}
| . |
| . .\
| . . 5. ¬a≥0
```

```
| . . 6. ¬b≥0
| . . ⊢  (a rem b) = 0
| . . | by RWH
| . . |    (LemmaC
| . . |     Thm* ∀a:{...0}, n:{...-1}. (a rem n) = -((-a) rem -n)
| . . |     {rem_3_to_1})
| . . |    0
| . . |
| . . ⊢  -((-a) rem -b) = 0  by Rewrite (HigherC (HypC 4)) 0
| . . |
| . . .....rewrite subgoal .....
| . . ⊢  -b | -a
| . .   by (BackThru
| . .       Thm* ∀a,b:ℤ. a | b ⟺ -a | b    {divides_invar_1})
| . .      THEN
| . .      (BackThru
| . .       Thm* ∀a,b:ℤ. a | b ⟺ a | -b    {divides_invar_2})
|
.\
. 1. a : ℤ
. 2. b : ℤ^-0
. 3. (a rem b) = 0
. ⊢  b | a  by Witness a ÷ b
. |
. ⊢  a = b·(a ÷ b)
. | by Rewrite
. |    (HigherC
. |     (LemmaC
. |      Thm* ∀a:ℤ, n:ℤ^-0. (a rem n) = a-(a ÷ n)·n    {rem_to_div}))
. |    3
. |
. 3. a-(a ÷ b)·b = 0
. ⊢  a = b·(a ÷ b)
.   by Using [`n`,((a ÷ b)·b)]
.      (FwdThru Thm* ∀a,b,n:ℤ. a = b ⟺ a+n = b+n    {add_mono_wrt_eq}
.       [3])
END
```