```
div_rem_unique  THM

⊢  ∀a:ℤ, n:ℤ^-0, q,r:ℤ.
|  a = q·n+r
|  ⇒
|  |r|<|n|
|  ⇒
|  (r<0 ⇒ a<0) ⇒ (r>0 ⇒ a>0) ⇒ q = (a ÷ n) & r = (a rem n)
| by Auto
|    THEN
|    (Inst
|     Thm* ∀a:ℤ, n:ℤ^-0.
|          a = (a ÷ n)·n+(a rem n)
|          & |a rem n|<|n|
|          & ((a rem n)<0 ⇒ a<0)
|          & ((a rem n)>0 ⇒ a>0)
|     {div_rem_properties}
|     [a;n])
|
1. a : ℤ
2. n : ℤ^-0
3. q : ℤ
4. r : ℤ
5. a = q·n+r
6. |r|<|n|
7. r<0 ⇒ a<0
8. r>0 ⇒ a>0
9. a = (a ÷ n)·n+(a rem n)
10. |a rem n|<|n|
11. (a rem n)<0 ⇒ a<0
12. (a rem n)>0 ⇒ a>0
⊢  q = (a ÷ n) & r = (a rem n)
| by ((RepeatFor 4 (MoveToConcl -1)) THEN (GenConcl ((a ÷ n) = q')))
|    THEN
|    (Thin -1)
|    THEN
|    (GenConcl ((a rem n) = r'))
|    THEN
|    (Thin -1)
|    THEN
|    (Unfold `guard` 0)
|
1. a : ℤ
2. n : ℤ^-0
3. q : ℤ
4. r : ℤ
5. a = q·n+r
6. |r|<|n|
7. r<0 ⇒ a<0
8. r>0 ⇒ a>0
9. q' : ℤ
10. r' : ℤ
⊢  a = q'·n+r'
|  ⇒
|  |r'|<|n| ⇒ (r'<0 ⇒ a<0) ⇒ (r'>0 ⇒ a>0) ⇒ q = q' & r = r'
```

```
| by (Analyze 0) THEN (Assert ((q-q')·n = r'-r))
|
|\
| .....assertion .....
| 1. a : ℤ
| 2. n : ℤ^-0
| 3. q : ℤ
| 4. r : ℤ
| 5. a = q·n+r
| 6. |r|<|n|
| 7. r<0 ⇒ a<0
| 8. r>0 ⇒ a>0
| 9. q' : ℤ
| 10. r' : ℤ
| 11. a = q'·n+r'
| ⊢  (q-q')·n = r'-r  by Auto
|
.\
. 1. a : ℤ
. 2. n : ℤ^-0
. 3. q : ℤ
. 4. r : ℤ
. 5. a = q·n+r
. 6. |r|<|n|
. 7. r<0 ⇒ a<0
. 8. r>0 ⇒ a>0
. 9. q' : ℤ
. 10. r' : ℤ
. 11. a = q'·n+r'
. 12. (q-q')·n = r'-r
. ⊢  |r'|<|n| ⇒ (r'<0 ⇒ a<0) ⇒ (r'>0 ⇒ a>0) ⇒ q = q' & r = r'
. | by Decide (q = q')
. |
. |\
. | 1. a : ℤ
. | 2. n : ℤ^-0
. | 3. q : ℤ
. | 4. r : ℤ
. | 5. a = q·n+r
. | 6. |r|<|n|
. | 7. r<0 ⇒ a<0
. | 8. r>0 ⇒ a>0
. | 9. q' : ℤ
. | 10. r' : ℤ
. | 11. a = q'·n+r'
. | 12. (q-q')·n = r'-r
. | 13. q = q'
. | ⊢  |r'|<|n| ⇒ (r'<0 ⇒ a<0) ⇒ (r'>0 ⇒ a>0) ⇒ q = q' & r = r'
. | | by Auto
. | |
. | 1. a : ℤ
. | 2. n : ℤ^-0
. | 3. q : ℤ
. | 4. r : ℤ
. | 5. a = q·n+r
```

```
. | 6. |r|<|n|
. | 7. r<0 ⇒ a<0
. | 8. r>0 ⇒ a>0
. | 9. q' : ℤ
. | 10. r' : ℤ
. | 11. a = q'·n+r'
. | 12. (q-q')·n = r'-r
. | 13. q = q'
. | 14. |r'|<|n|
. | 15. r'<0 ⇒ a<0
. | 16. r'>0 ⇒ a>0
. | ⊢  r = r'  by Subst (q-q' = 0) -5
. |
. .\
. . 1. a : ℤ
. . 2. n : ℤ^-0
. . 3. q : ℤ
. . 4. r : ℤ
. . 5. a = q·n+r
. . 6. |r|<|n|
. . 7. r<0 ⇒ a<0
. . 8. r>0 ⇒ a>0
. . 9. q' : ℤ
. . 10. r' : ℤ
. . 11. a = q'·n+r'
. . 12. (q-q')·n = r'-r
. . 13. ¬q = q'
. . ⊢  |r'|<|n| ⇒ (r'<0 ⇒ a<0) ⇒ (r'>0 ⇒ a>0) ⇒ q = q' & r = r'
. . | by Assert (|n|≤|r'-r|)
. . |
. . |\
. . | .....assertion .....
. . | 1. a : ℤ
. . | 2. n : ℤ^-0
. . | 3. q : ℤ
. . | 4. r : ℤ
. . | 5. a = q·n+r
. . | 6. |r|<|n|
. . | 7. r<0 ⇒ a<0
. . | 8. r>0 ⇒ a>0
. . | 9. q' : ℤ
. . | 10. r' : ℤ
. . | 11. a = q'·n+r'
. . | 12. (q-q')·n = r'-r
. . | 13. ¬q = q'
. . | ⊢  |n|≤|r'-r|  by RevHypSubst -2 0
. . | |
. . | 1. a : ℤ
. . | 2. n : ℤ^-0
. . | 3. q : ℤ
. . | 4. r : ℤ
. . | 5. a = q·n+r
. . | 6. |r|<|n|
. . | 7. r<0 ⇒ a<0
. . | 8. r>0 ⇒ a>0
```

```
. . | 9. q' : ℤ
. . | 10. r' : ℤ
. . | 11. a = q'·n+r'
. . | 12. (q-q')·n = r'-r
. . | 13. ¬q = q'
. . | ⊢ |n|≤|(q-q')·n|  by GenConcl (q-q' = x)
. . | |
. . | 1. a : ℤ
. . | 2. n : ℤ⁻⁰
. . | 3. q : ℤ
. . | 4. r : ℤ
. . | 5. a = q·n+r
. . | 6. |r|<|n|
. . | 7. r<0 ⇒ a<0
. . | 8. r>0 ⇒ a>0
. . | 9. q' : ℤ
. . | 10. r' : ℤ
. . | 11. a = q'·n+r'
. . | 12. (q-q')·n = r'-r
. . | 13. ¬q = q'
. . | 14. x : ℤ⁻⁰
. . | 15. q-q' = x
. . | ⊢ |n|≤|x·n|  by Lemmaize []
. . | |
. . | 1. n : ℤ⁻⁰
. . | 2. x : ℤ⁻⁰
. . | ⊢ |n|≤|x·n|  by Subst (|x·n| = |x|·|n|) 0
. . | |
. . | |\
. . | | .....equality .....
. . | | 1. n : ℤ⁻⁰
. . | | 2. x : ℤ⁻⁰
. . | | ⊢ |x·n| = |x|·|n|
. . | |   by BackThru Thm* ∀a,b:ℤ. |a·b| = |a|·|b|    {absval_mul}
. . | |
. . | .\
. . | . 1. n : ℤ⁻⁰
. . | . 2. x : ℤ⁻⁰
. . | . ⊢ |n|≤|x|·|n|
. . | . | by Inst
. . | . |    Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b    {mul_preserves_le}
. . | . |    [1;|x|;|n|]
. . | . |
. . | . .....antecedent .....
. . | . 1. ℤ⁻⁰
. . | . 2. x : ℤ⁻⁰
. . | . ⊢ 1≤|x|  by (Unfold `absval` 0) THEN SplitOnConclITE
. . |
. . .\
. . . 1. a : ℤ
. . . 2. n : ℤ⁻⁰
. . . 3. q : ℤ
. . . 4. r : ℤ
. . . 5. a = q·n+r
. . . 6. |r|<|n|
```

```
. . . 7. r<0 ⇒ a<0
. . . 8. r>0 ⇒ a>0
. . . 9. q' : ℤ
. . . 10. r' : ℤ
. . . 11. a = q'·n+r'
. . . 12. (q-q')·n = r'-r
. . . 13. ¬q = q'
. . . 14. |n|≤|r'-r|
. . . ⊢  |r'|<|n| ⇒ (r'<0 ⇒ a<0) ⇒ (r'>0 ⇒ a>0) ⇒ q = q' & r = r'
. . .   by (RepeatFor 3 (Analyze 0)) THEN (Assert False)
. . .      THEN
. . .      (Try Trivial)
. . .      THEN
. . .      (RepeatFor 4 (MoveToConcl -1))
. . .      THEN
. . .      (MoveToConcl 6)
. . .      THEN
. . .      (Unfold `absval` 0)
. . .      THEN
. . .      (Repeat SplitOnConclITE)
. . .      THEN
. . .      (ImplicationsIf Auto)
END
```