```
div_floor_mod_unique  THM

⊢  ∀a:ℤ, n:ℕ+, q:ℤ, r:ℕ.
|  a = q·n+r ⇒ r<n ⇒ q = (a ÷↓ n) & r = (a mod n)
| by Auto
|    THEN
|    (Inst
|     Thm* ∀a:ℤ, n:ℕ+. a = (a ÷↓ n)·n+(a mod n) & (a mod n)<n
|     {div_floor_mod_properties}
|     [a;n])
|
1. a : ℤ
2. n : ℕ+
3. q : ℤ
4. r : ℕ
5. a = q·n+r
6. r<n
7. a = (a ÷↓ n)·n+(a mod n)
8. (a mod n)<n
⊢  q = (a ÷↓ n) & r = (a mod n)
| by ((RepeatFor 2 (MoveToConcl -1)) THEN (GenConcl ((a ÷↓ n) = q')))
|    THEN
|    (Thin -1)
|    THEN
|    (GenConcl ((a mod n) = r'))
|    THEN
|    (Thin -1)
|    THEN
|    (Unfold `guard` 0)
|
1. a : ℤ
2. n : ℕ+
3. q : ℤ
4. r : ℕ
5. a = q·n+r
6. r<n
7. q' : ℤ
8. r' : ℕ
⊢  a = q'·n+r' ⇒ r'<n ⇒ q = q' & r = r'
| by (Analyze 0) THEN (Assert ((q-q')·n = r'-r))
|
|\
| .....assertion .....
| 1. a : ℤ
| 2. n : ℕ+
| 3. q : ℤ
| 4. r : ℕ
| 5. a = q·n+r
| 6. r<n
| 7. q' : ℤ
| 8. r' : ℕ
| 9. a = q'·n+r'
| ⊢  (q-q')·n = r'-r  by Auto
|
.\
```

```
. 1. a : ℤ
. 2. n : ℕ+
. 3. q : ℤ
. 4. r : ℕ
. 5. a = q·n+r
. 6. r<n
. 7. q' : ℤ
. 8. r' : ℕ
. 9. a = q'·n+r'
. 10. (q-q')·n = r'-r
. ⊢  r'<n ⇒ q = q' & r = r'  by Decide (q = q')
. |
. |\
. | 1. a : ℤ
. | 2. n : ℕ+
. | 3. q : ℤ
. | 4. r : ℕ
. | 5. a = q·n+r
. | 6. r<n
. | 7. q' : ℤ
. | 8. r' : ℕ
. | 9. a = q'·n+r'
. | 10. (q-q')·n = r'-r
. | 11. q = q'
. | ⊢  r'<n ⇒ q = q' & r = r'  by Auto
. | |
. | 1. a : ℤ
. | 2. n : ℕ+
. | 3. q : ℤ
. | 4. r : ℕ
. | 5. a = q·n+r
. | 6. r<n
. | 7. q' : ℤ
. | 8. r' : ℕ
. | 9. a = q'·n+r'
. | 10. (q-q')·n = r'-r
. | 11. q = q'
. | 12. r'<n
. | ⊢  r = r'  by Subst (q-q' = 0) -3
. |
. .\
. . 1. a : ℤ
. . 2. n : ℕ+
. . 3. q : ℤ
. . 4. r : ℕ
. . 5. a = q·n+r
. . 6. r<n
. . 7. q' : ℤ
. . 8. r' : ℕ
. . 9. a = q'·n+r'
. . 10. (q-q')·n = r'-r
. . 11. ¬q = q'
. . ⊢  r'<n ⇒ q = q' & r = r'  by Assert (|n|≤|r'-r|)
. . |
. . |\
```

```
. . | .....assertion .....
. . | 1. a : ℤ
. . | 2. n : ℕ+
. . | 3. q : ℤ
. . | 4. r : ℕ
. . | 5. a = q·n+r
. . | 6. r<n
. . | 7. q' : ℤ
. . | 8. r' : ℕ
. . | 9. a = q'·n+r'
. . | 10. (q-q')·n = r'-r
. . | 11. ¬q = q'
. . | ⊢  |n|≤|r'-r|  by RevHypSubst -2 0
. . | |
. . | 1. a : ℤ
. . | 2. n : ℕ+
. . | 3. q : ℤ
. . | 4. r : ℕ
. . | 5. a = q·n+r
. . | 6. r<n
. . | 7. q' : ℤ
. . | 8. r' : ℕ
. . | 9. a = q'·n+r'
. . | 10. (q-q')·n = r'-r
. . | 11. ¬q = q'
. . | ⊢  |n|≤|(q-q')·n|  by GenConcl (q-q' = x)
. . | |
. . | 1. a : ℤ
. . | 2. n : ℕ+
. . | 3. q : ℤ
. . | 4. r : ℕ
. . | 5. a = q·n+r
. . | 6. r<n
. . | 7. q' : ℤ
. . | 8. r' : ℕ
. . | 9. a = q'·n+r'
. . | 10. (q-q')·n = r'-r
. . | 11. ¬q = q'
. . | 12. x : ℤ-0
. . | 13. q-q' = x
. . | ⊢  |n|≤|x·n|  by Lemmaize []
. . | |
. . | 1. n : ℕ+
. . | 2. x : ℤ-0
. . | ⊢  |n|≤|x·n|  by Subst (|x·n| = |x|·|n|) 0
. . | |
. . | |\
. . | | .....equality .....
. . | | 1. n : ℕ+
. . | | 2. x : ℤ-0
. . | | ⊢  |x·n| = |x|·|n|
. . | |    by BackThru Thm* ∀a,b:ℤ. |a·b| = |a|·|b|    {absval_mul}
. . | |
. . | .\
. . | . 1. n : ℕ+
```

```
. . | . 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. ℕ+
. . | . 2. x : ℤ⁻⁰
. . | . ⊢  1≤|x|  by (Unfold `absval` 0) THEN SplitOnConclITE
. . |
. . .\
. . . 1. a : ℤ
. . . 2. n : ℕ+
. . . 3. q : ℤ
. . . 4. r : ℕ
. . . 5. a = q·n+r
. . . 6. r<n
. . . 7. q' : ℤ
. . . 8. r' : ℕ
. . . 9. a = q'·n+r'
. . . 10. (q-q')·n = r'-r
. . . 11. ¬q = q'
. . . 12. |n|≤|r'-r|
. . . ⊢  r'<n ⇒ q = q' & r = r'
. . .   by (Analyze 0) THEN (Assert False) THEN (Try Trivial)
. . .      THEN
. . .      (RepeatFor 2 (MoveToConcl -1))
. . .      THEN
. . .      (MoveToConcl 6)
. . .      THEN
. . .      (Unfold `absval` 0)
. . .      THEN
. . .      (Repeat SplitOnConclITE)
. . .      THEN
. . .      (ImplicationsIf Auto)
END
```