```
rem_mul  THM

⊢  ∀x,y:ℤ, n:ℤ⁻⁰. ((x·y) rem n) = (((x rem n)·(y rem n)) 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}
|       [x;n]))
|     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}
|      [y;n])
|     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}
|      [(x rem n)·(y rem n);n]))
|    THEN
|    RepDHyps
|
1. x : ℤ
2. y : ℤ
3. n : ℤ⁻⁰
4. x = (x ÷ n)·n+(x rem n)
5. |x rem n|<|n|
6. (x rem n)<0 ⇒ x<0
7. (x rem n)>0 ⇒ x>0
8. y = (y ÷ n)·n+(y rem n)
9. |y rem n|<|n|
10. (y rem n)<0 ⇒ y<0
11. (y rem n)>0 ⇒ y>0
12. (x rem n)·(y rem n)
|   =
|   (((x rem n)·(y rem n)) ÷ n)·n+(((x rem n)·(y rem n)) rem n)
13. |((x rem n)·(y rem n)) rem n|<|n|
14. (((x rem n)·(y rem n)) rem n)<0 ⇒ (x rem n)·(y rem n)<0
15. (((x rem n)·(y rem n)) rem n)>0 ⇒ (x rem n)·(y rem n)>0
⊢  ((x·y) rem n) = (((x rem n)·(y rem n)) rem n)
| by Inst
|    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)
|     {div_rem_unique}
|     [x·y
|     ;n
|     ;(x ÷ n)·(y ÷ n)·n+(x ÷ n)·(y rem n)+(x rem n)·(y ÷ n)
|      +(((x rem n)·(y rem n)) ÷ n)
|     ;((x rem n)·(y rem n)) rem n]
|
|\
| .....antecedent .....
| 1. x : ℤ
| 2. y : ℤ
| 3. n : ℤ⁻⁰
| 4. x = (x ÷ n)·n+(x rem n)
| 5. |x rem n|<|n|
| 6. (x rem n)<0 ⇒ x<0
| 7. (x rem n)>0 ⇒ x>0
| 8. y = (y ÷ n)·n+(y rem n)
| 9. |y rem n|<|n|
| 10. (y rem n)<0 ⇒ y<0
| 11. (y rem n)>0 ⇒ y>0
| 12. (x rem n)·(y rem n)
|      =
|      (((x rem n)·(y rem n)) ÷ n)·n+(((x rem n)·(y rem n)) rem n)
| 13. |((x rem n)·(y rem n)) rem n|<|n|
| 14. (((x rem n)·(y rem n)) rem n)<0 ⇒ (x rem n)·(y rem n)<0
| 15. (((x rem n)·(y rem n)) rem n)>0 ⇒ (x rem n)·(y rem n)>0
| ⊢  x·y
|     =
|     ((x ÷ n)·(y ÷ n)·n+(x ÷ n)·(y rem n)+(x rem n)·(y ÷ n)
|      +(((x rem n)·(y rem n)) ÷ n))·n+(((x rem n)·(y rem n)) rem n)
|    by (Subst (x·y = ((x ÷ n)·n+(x rem n))·((y ÷ n)·n+(y rem n))) 0)
|       THEN
|       (All ArithSimp)
|
|\
| 1. x : ℤ
| 2. y : ℤ
| 3. n : ℤ⁻⁰
| 4. x = (x ÷ n)·n+(x rem n)
| 5. |x rem n|<|n|
| 6. (x rem n)<0 ⇒ x<0
| 7. (x rem n)>0 ⇒ x>0
| 8. y = (y ÷ n)·n+(y rem n)
| 9. |y rem n|<|n|
| 10. (y rem n)<0 ⇒ y<0
| 11. (y rem n)>0 ⇒ y>0
| 12. (x rem n)·(y rem n)
|      =
|      (((x rem n)·(y rem n)) ÷ n)·n+(((x rem n)·(y rem n)) rem n)
| 13. |((x rem n)·(y rem n)) rem n|<|n|
| 14. (((x rem n)·(y rem n)) rem n)<0 ⇒ (x rem n)·(y rem n)<0
```

```
| 15. (((x rem n)·(y rem n)) rem n)>0 ⇒ (x rem n)·(y rem n)>0
| 16. (((x rem n)·(y rem n)) rem n)<0
| ⊢  x·y<0
|   by ThinTrivial
|      THEN
|      (RWO
|       Thm* ∀a,b:ℤ. a·b<0 ⟺ a<0 & b>0 ∨ a>0 & b<0
|       {neg_mul_arg_bounds}
|       0)
|      THEN
|      (RWO
|       Thm* ∀a,b:ℤ. a·b<0 ⟺ a<0 & b>0 ∨ a>0 & b<0
|       {neg_mul_arg_bounds}
|       -1)
|      THEN
|      (ParallelOp -1)
|      THEN
|      (ParallelOp -1)
|      THEN
|      EasyHyp
|
.\
. 1. x : ℤ
. 2. y : ℤ
. 3. n : ℤ⁻⁰
. 4. x = (x ÷ n)·n+(x rem n)
. 5. |x rem n|<|n|
. 6. (x rem n)<0 ⇒ x<0
. 7. (x rem n)>0 ⇒ x>0
. 8. y = (y ÷ n)·n+(y rem n)
. 9. |y rem n|<|n|
. 10. (y rem n)<0 ⇒ y<0
. 11. (y rem n)>0 ⇒ y>0
. 12. (x rem n)·(y rem n)
.     =
.     (((x rem n)·(y rem n)) ÷ n)·n+(((x rem n)·(y rem n)) rem n)
. 13. |((x rem n)·(y rem n)) rem n|<|n|
. 14. (((x rem n)·(y rem n)) rem n)<0 ⇒ (x rem n)·(y rem n)<0
. 15. (((x rem n)·(y rem n)) rem n)>0 ⇒ (x rem n)·(y rem n)>0
. 16. (((x rem n)·(y rem n)) rem n)>0
. ⊢  x·y>0
.   by ThinTrivial
.      THEN
.      (RWO
.       Thm* ∀a,b:ℤ. a·b>0 ⟺ a>0 & b>0 ∨ a<0 & b<0
.       {pos_mul_arg_bounds}
.       0)
.      THEN
.      (RWO
.       Thm* ∀a,b:ℤ. a·b>0 ⟺ a>0 & b>0 ∨ a<0 & b<0
.       {pos_mul_arg_bounds}
.       -1)
.      THEN
.      (ParallelOp -1)
.      THEN
```

```
.       (ParallelOp -1)
.       THEN
.       EasyHyp
END
```