```
mod_mul  THM

⊢  ∀x,y:ℤ, n:ℕ+ . ((x·y) mod n) = (((x mod n)·(y mod n)) 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}
|       [x;n]))
|     THEN
|     (Inst
|      Thm* ∀a:ℤ, n:ℕ+ . a = (a ÷↓ n)·n+(a mod n) & (a mod n)<n
|      {div_floor_mod_properties}
|      [y;n])
|     THEN
|     (Inst
|      Thm* ∀a:ℤ, n:ℕ+ . a = (a ÷↓ n)·n+(a mod n) & (a mod n)<n
|      {div_floor_mod_properties}
|      [(x mod n)·(y mod n);n]))
|    THEN
|    RepDHyps
|
1. x : ℤ
2. y : ℤ
3. n : ℕ+
4. x = (x ÷↓ n)·n+(x mod n)
5. (x mod n)<n
6. y = (y ÷↓ n)·n+(y mod n)
7. (y mod n)<n
8. (x mod n)·(y mod n)
|  =
|  (((x mod n)·(y mod n)) ÷↓ n)·n+(((x mod n)·(y mod n)) mod n)
9. (((x mod n)·(y mod n)) mod n)<n
⊢  ((x·y) mod n) = (((x mod n)·(y mod n)) mod n)
| by Inst
|    Thm* ∀a:ℤ, n:ℕ+, q:ℤ, r:ℕ.
|         a = q·n+r ⇒ r<n ⇒ q = (a ÷↓ n) & r = (a mod n)
|    {div_floor_mod_unique}
|    [x·y
|    ;n
|    ;(x ÷↓ n)·(y ÷↓ n)·n+(x ÷↓ n)·(y mod n)+(x mod n)·(y ÷↓ n)
|     +(((x mod n)·(y mod n)) ÷↓ n)
|    ;((x mod n)·(y mod n)) mod n]
|
.....antecedent .....
1. x : ℤ
2. y : ℤ
3. n : ℕ+
4. x = (x ÷↓ n)·n+(x mod n)
5. (x mod n)<n
6. y = (y ÷↓ n)·n+(y mod n)
7. (y mod n)<n
8. (x mod n)·(y mod n)
   =
   (((x mod n)·(y mod n)) ÷↓ n)·n+(((x mod n)·(y mod n)) mod n)
```

```
9. (((x mod n)·(y mod n)) mod n)<n
⊢  x·y
   =
   ((x ÷↓ n)·(y ÷↓ n)·n+(x ÷↓ n)·(y mod n)+(x mod n)·(y ÷↓ n)
    +(((x mod n)·(y mod n)) ÷↓ n))·n+(((x mod n)·(y mod n)) mod n)
  by (Subst (x·y = ((x ÷↓ n)·n+(x mod n))·((y ÷↓ n)·n+(y mod n))) 0)
     THEN
     (All ArithSimp)
END
```