```
sqrt_prime_irrational  THM

⊢  ∀p:ℤ⁻⁰. prime(p) ⇒ (∀m,n:ℕ. m·m = p·n·n ⇒ n = 0)
| by (RepeatFor 2 (Analyze 0)) THEN (Decide (0<p))
|
|\
| 1. p : ℤ⁻⁰
| 2. prime(p)
| 3. 0<p
| ⊢  ∀m,n:ℕ. m·m = p·n·n ⇒ n = 0
| | by CompleteInductionOnNat THEN SupposeNot
| |
| 1. p : ℤ⁻⁰
| 2. prime(p)
| 3. 0<p
| 4. m : ℕ
| 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| 6. n : ℕ
| 7. m·m = p·n·n
| 8. ¬n = 0
| ⊢  n = 0
| | by Inst
| |    Thm* ∀a:ℤ, n:ℕ⁺. a = (a ÷↓ n)·n+(a mod n) & (a mod n)<n
| |    {div_floor_mod_properties}
| |    [m;p]
| |
| 1. p : ℤ⁻⁰
| 2. prime(p)
| 3. 0<p
| 4. m : ℕ
| 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| 6. n : ℕ
| 7. m·m = p·n·n
| 8. ¬n = 0
| 9. m = (m ÷↓ p)·p+(m mod p)
| 10. (m mod p)<p
| ⊢  n = 0  by InstHyp [n] 5
| |
| |\
| | .....antecedent .....
| | 1. p : ℤ⁻⁰
| | 2. prime(p)
| | 3. 0<p
| | 4. m : ℕ
| | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| | 6. n : ℕ
| | 7. m·m = p·n·n
| | 8. ¬n = 0
| | 9. m = (m ÷↓ p)·p+(m mod p)
| | 10. (m mod p)<p
| | ⊢  n<m  by Decide (m≤n)
| | |
| | 1. p : ℤ⁻⁰
| | 2. prime(p)
| | 3. 0<p
```

```
| | 4. m : ℕ
| | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| | 6. n : ℕ
| | 7. m·m = p·n·n
| | 8. ¬n = 0
| | 9. m = (m ÷↓ p)·p+(m mod p)
| | 10. (m mod p)<p
| | 11. m≤n
| | ⊢  n<m  by Assert (0<n·n)
| | |
| | |\
| | | .....assertion .....
| | | 1. p : ℤ^-0
| | | 2. prime(p)
| | | 3. 0<p
| | | 4. m : ℕ
| | | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| | | 6. n : ℕ
| | | 7. m·m = p·n·n
| | | 8. ¬n = 0
| | | 9. m = (m ÷↓ p)·p+(m mod p)
| | | 10. (m mod p)<p
| | | 11. m≤n
| | | ⊢  0<n·n  by BackThru Thm* ∀a,b:ℕ+. 0<a·b    {mul_bounds_1b}
| | |
| | .\
| | . 1. p : ℤ^-0
| | . 2. prime(p)
| | . 3. 0<p
| | . 4. m : ℕ
| | . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| | . 6. n : ℕ
| | . 7. m·m = p·n·n
| | . 8. ¬n = 0
| | . 9. m = (m ÷↓ p)·p+(m mod p)
| | . 10. (m mod p)<p
| | . 11. m≤n
| | . 12. 0<n·n
| | . ⊢  n<m
| | . | by (Inst
| | . |     Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b    {mul_preserves_le}
| | . |     [m;n;n])
| | . |    THEN
| | . |    (Inst
| | . |     Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b    {mul_preserves_le}
| | . |     [m;n;m])
| | . |    THEN
| | . |    (Inst Thm* ∀a,b:ℤ. a·b = b·a    {mul_com} [m;n])
| | . |
| | . 1. p : ℤ^-0
| | . 2. prime(p)
| | . 3. 0<p
| | . 4. m : ℕ
| | . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| | . 6. n : ℕ
```

```
| | . 7. m·m = p·n·n
| | . 8. ¬n = 0
| | . 9. m = (m ÷↓ p)·p+(m mod p)
| | . 10. (m mod p)<p
| | . 11. m≤n
| | . 12. 0<n·n
| | . 13. n·m≤n·n
| | . 14. m·m≤m·n
| | . 15. m·n = n·m
| | . ⊢  n<m
| | . | by Inst Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b    {mul_preserves_le}
| | . |    [2;p;n·n]
| | . |
| | . .....antecedent .....
| | . 1. p : ℤ^-0
| | . 2. prime(p)
| | . 3. 0<p
| | . 4. m : ℕ
| | . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| | . 6. n : ℕ
| | . 7. m·m = p·n·n
| | . 8. ¬n = 0
| | . 9. m = (m ÷↓ p)·p+(m mod p)
| | . 10. (m mod p)<p
| | . 11. m≤n
| | . 12. 0<n·n
| | . 13. n·m≤n·n
| | . 14. m·m≤m·n
| | . 15. m·n = n·m
| | . ⊢  2≤p  by Decide (p = 1)
| | . |
| | . 1. p : ℤ^-0
| | . 2. prime(p)
| | . 3. 0<p
| | . 4. m : ℕ
| | . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| | . 6. n : ℕ
| | . 7. m·m = p·n·n
| | . 8. ¬n = 0
| | . 9. m = (m ÷↓ p)·p+(m mod p)
| | . 10. (m mod p)<p
| | . 11. m≤n
| | . 12. 0<n·n
| | . 13. n·m≤n·n
| | . 14. m·m≤m·n
| | . 15. m·n = n·m
| | . 16. p = 1
| | . ⊢  2≤p  by Assert (¬prime(1))
| | . |
| | . |\
| | . | .....assertion .....
| | . | 1. p : ℤ^-0
| | . | 2. prime(p)
| | . | 3. 0<p
| | . | 4. m : ℕ
```

```
| | . | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| | . | 6. n : ℕ
| | . | 7. m·m = p·n·n
| | . | 8. ¬n = 0
| | . | 9. m = (m ÷↓ p)·p+(m mod p)
| | . | 10. (m mod p)<p
| | . | 11. m≤n
| | . | 12. 0<n·n
| | . | 13. n·m≤n·n
| | . | 14. m·m≤m·n
| | . | 15. m·n = n·m
| | . | 16. p = 1
| | . | ⊢  ¬prime(1)
| | . | | by (Analyze 0) THEN (Analyze -1) THEN (Analyze -1)
| | . | |    THEN
| | . | |    (Analyze -2)
| | . | |
| | . | 1. p : ℤ⁻⁰
| | . | 2. prime(p)
| | . | 3. 0<p
| | . | 4. m : ℕ
| | . | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| | . | 6. n : ℕ
| | . | 7. m·m = p·n·n
| | . | 8. ¬n = 0
| | . | 9. m = (m ÷↓ p)·p+(m mod p)
| | . | 10. (m mod p)<p
| | . | 11. m≤n
| | . | 12. 0<n·n
| | . | 13. n·m≤n·n
| | . | 14. m·m≤m·n
| | . | 15. m·n = n·m
| | . | 16. p = 1
| | . | 17. ¬1 = 0
| | . | 18. ∀b,c:ℤ. (1 | (b·c)) ⇒ (1 | b) ∨ (1 | c)
| | . | ⊢  1 ∼ 1  by (Analyze 0) THEN Witness 1
| | . |

| | . .\
| | . . 1. p : ℤ⁻⁰
| | . . 2. prime(p)
| | . . 3. 0<p
| | . . 4. m : ℕ
| | . . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| | . . 6. n : ℕ
| | . . 7. m·m = p·n·n
| | . . 8. ¬n = 0
| | . . 9. m = (m ÷↓ p)·p+(m mod p)
| | . . 10. (m mod p)<p
| | . . 11. m≤n
| | . . 12. 0<n·n
| | . . 13. n·m≤n·n
| | . . 14. m·m≤m·n
| | . . 15. m·n = n·m
| | . . 16. p = 1
| | . . 17. ¬prime(1)
```

```
| | . . ⊢  2≤p  by HypSubst -2 2
| |
| .\
| . 1. p : ℤ^{-0}
| . 2. prime(p)
| . 3. 0<p
| . 4. m : ℕ
| . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . 6. n : ℕ
| . 7. m·m = p·n·n
| . 8. ¬n = 0
| . 9. m = (m ÷↓ p)·p+(m mod p)
| . 10. (m mod p)<p
| . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . ⊢  n = 0  by HypSubst -3 -5
| . |
| . 1. p : ℤ^{-0}
| . 2. prime(p)
| . 3. 0<p
| . 4. m : ℕ
| . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . 6. n : ℕ
| . 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . 8. ¬n = 0
| . 9. m = (m ÷↓ p)·p+(m mod p)
| . 10. (m mod p)<p
| . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . ⊢  n = 0  by ReduceMod p -5
| . |
| . 1. p : ℤ^{-0}
| . 2. prime(p)
| . 3. 0<p
| . 4. m : ℕ
| . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . 6. n : ℕ
| . 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . 8. ¬n = 0
| . 9. m = (m ÷↓ p)·p+(m mod p)
| . 10. (m mod p)<p
| . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . 12. (((m mod p)·(m mod p)) mod p) = 0
| . ⊢  n = 0  by RWO "elim_divides<" -1
| . |
| . 1. p : ℤ^{-0}
| . 2. prime(p)
| . 3. 0<p
| . 4. m : ℕ
| . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . 6. n : ℕ
| . 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . 8. ¬n = 0
| . 9. m = (m ÷↓ p)·p+(m mod p)
| . 10. (m mod p)<p
| . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . 12. p | ((m mod p)·(m mod p))
```

```
| . ⊢  n = 0  by Assert (p | (m mod p))
| . |
| . |\
| . | .....assertion .....
| . | 1. p : ℤ^-0
| . | 2. prime(p)
| . | 3. 0<p
| . | 4. m : ℕ
| . | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . | 6. n : ℕ
| . | 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . | 8. ¬n = 0
| . | 9. m = (m ÷↓ p)·p+(m mod p)
| . | 10. (m mod p)<p
| . | 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . | 12. p | ((m mod p)·(m mod p))
| . | ⊢  p | (m mod p)
| . | | by (Unfold ‘prime‘ 2) THEN RepD
| . | |    THEN
| . | |    (InstHyp [m mod p;m mod p] 4)
| . | |
| . | 1. p : ℤ^-0
| . | 2. ¬p = 0
| . | 3. ¬(p ∼ 1)
| . | 4. ∀b,c:ℤ. (p | (b·c)) ⇒ (p | b) ∨ (p | c)
| . | 5. 0<p
| . | 6. m : ℕ
| . | 7. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . | 8. n : ℕ
| . | 9. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . | 10. ¬n = 0
| . | 11. m = (m ÷↓ p)·p+(m mod p)
| . | 12. (m mod p)<p
| . | 13. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . | 14. p | ((m mod p)·(m mod p))
| . | 15. (p | (m mod p)) ∨ (p | (m mod p))
| . | ⊢  p | (m mod p)  by (Analyze -1) THEN Trivial
| . |
| . .\
| . . 1. p : ℤ^-0
| . . 2. prime(p)
| . . 3. 0<p
| . . 4. m : ℕ
| . . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . 6. n : ℕ
| . . 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . 8. ¬n = 0
| . . 9. m = (m ÷↓ p)·p+(m mod p)
| . . 10. (m mod p)<p
| . . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . 12. p | ((m mod p)·(m mod p))
| . . 13. p | (m mod p)
| . . ⊢  n = 0  by (Unfold ‘divides‘ -1) THEN ExRepD
| . . |
| . . 1. p : ℤ^-0
```

```
| . . 2. prime(p)
| . . 3. 0<p
| . . 4. m : ℕ
| . . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . 6. n : ℕ
| . . 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . 8. ¬n = 0
| . . 9. m = (m ÷↓ p)·p+(m mod p)
| . . 10. (m mod p)<p
| . . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . 12. p | ((m mod p)·(m mod p))
| . . 13. c : ℤ
| . . 14. (m mod p) = p·c
| . . ⊢  n = 0
| . . | by Inst
| . . |    Thm* ∀a,b:ℤ, n:ℕ+. n·a<n·b ⇒ a<b    {mul_cancel_in_lt}
| . . |    [c;1;p]
| . . |
| . . 1. p : ℤ-0
| . . 2. prime(p)
| . . 3. 0<p
| . . 4. m : ℕ
| . . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . 6. n : ℕ
| . . 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . 8. ¬n = 0
| . . 9. m = (m ÷↓ p)·p+(m mod p)
| . . 10. (m mod p)<p
| . . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . 12. p | ((m mod p)·(m mod p))
| . . 13. c : ℤ
| . . 14. (m mod p) = p·c
| . . 15. c<1
| . . ⊢  n = 0  by Decide (c<0)
| . . |
| . . |\
| . . | 1. p : ℤ-0
| . . | 2. prime(p)
| . . | 3. 0<p
| . . | 4. m : ℕ
| . . | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . | 6. n : ℕ
| . . | 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . | 8. ¬n = 0
| . . | 9. m = (m ÷↓ p)·p+(m mod p)
| . . | 10. (m mod p)<p
| . . | 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . | 12. p | ((m mod p)·(m mod p))
| . . | 13. c : ℤ
| . . | 14. (m mod p) = p·c
| . . | 15. c<1
| . . | 16. c<0
| . . | ⊢  n = 0  by Assert (p·c<0)
| . . | |
| . . | |\
```

```
| . . | | .....assertion .....
| . . | | 1. p : ℤ⁻⁰
| . . | | 2. prime(p)
| . . | | 3. 0<p
| . . | | 4. m : ℕ
| . . | | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . | | 6. n : ℕ
| . . | | 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . | | 8. ¬n = 0
| . . | | 9. m = (m ÷↓ p)·p+(m mod p)
| . . | | 10. (m mod p)<p
| . . | | 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . | | 12. p | ((m mod p)·(m mod p))
| . . | | 13. c : ℤ
| . . | | 14. (m mod p) = p·c
| . . | | 15. c<1
| . . | | 16. c<0
| . . | | ⊢  p·c<0
| . . | |   by (BackThru
| . . | |       Thm* ∀a,b:ℤ. a·b<0 ⟺ a<0 & b>0 ∨ a>0 & b<0
| . . | |       {neg_mul_arg_bounds})
| . . | |      THEN
| . . | |      OrRight
| . . | |
| . . | .\
| . . | . 1. p : ℤ⁻⁰
| . . | . 2. prime(p)
| . . | . 3. 0<p
| . . | . 4. m : ℕ
| . . | . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . | . 6. n : ℕ
| . . | . 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . | . 8. ¬n = 0
| . . | . 9. m = (m ÷↓ p)·p+(m mod p)
| . . | . 10. (m mod p)<p
| . . | . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . | . 12. p | ((m mod p)·(m mod p))
| . . | . 13. c : ℤ
| . . | . 14. (m mod p) = p·c
| . . | . 15. c<1
| . . | . 16. c<0
| . . | . 17. p·c<0
| . . | . ⊢  n = 0  by Auto
| . . |
| . . .\
| . . . 1. p : ℤ⁻⁰
| . . . 2. prime(p)
| . . . 3. 0<p
| . . . 4. m : ℕ
| . . . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . . 6. n : ℕ
| . . . 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . . 8. ¬n = 0
| . . . 9. m = (m ÷↓ p)·p+(m mod p)
| . . . 10. (m mod p)<p
```

```
| . . . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . . 12. p | ((m mod p)·(m mod p))
| . . . 13. c : ℤ
| . . . 14. (m mod p) = p·c
| . . . 15. c<1
| . . . 16. ¬c<0
| . . . ⊢  n = 0  by (Subst (c = 0) -3) THEN (ArithSimp -3)
| . . . |
| . . . 1. p : ℤ^-0
| . . . 2. prime(p)
| . . . 3. 0<p
| . . . 4. m : ℕ
| . . . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . . 6. n : ℕ
| . . . 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . . 8. ¬n = 0
| . . . 9. m = (m ÷↓ p)·p+(m mod p)
| . . . 10. (m mod p)<p
| . . . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . . 12. p | ((m mod p)·(m mod p))
| . . . 13. c : ℤ
| . . . 14. (m mod p) = 0
| . . . 15. c<1
| . . . 16. ¬c<0
| . . . ⊢  n = 0  by InstHyp [m ÷↓ p] -6
| . . . |
| . . . |\
| . . . | .....wf .....
| . . . | 1. p : ℤ^-0
| . . . | 2. prime(p)
| . . . | 3. 0<p
| . . . | 4. m : ℕ
| . . . | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . . | 6. n : ℕ
| . . . | 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . . | 8. ¬n = 0
| . . . | 9. m = (m ÷↓ p)·p+(m mod p)
| . . . | 10. (m mod p)<p
| . . . | 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . . | 12. p | ((m mod p)·(m mod p))
| . . . | 13. c : ℤ
| . . . | 14. (m mod p) = 0
| . . . | 15. c<1
| . . . | 16. ¬c<0
| . . . | ⊢  (m ÷↓ p) ∈ ℕ  by Auto
| . . . | |
| . . . | .....set predicate .....
| . . . | 1. p : ℤ^-0
| . . . | 2. prime(p)
| . . . | 3. 0<p
| . . . | 4. m : ℕ
| . . . | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . . | 6. n : ℕ
| . . . | 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . . | 8. ¬n = 0
```

```
| . . . | 9. m = (m ÷↓ p)·p+(m mod p)
| . . . | 10. (m mod p)<p
| . . . | 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . . | 12. p | ((m mod p)·(m mod p))
| . . . | 13. c : ℤ
| . . . | 14. (m mod p) = 0
| . . . | 15. c<1
| . . . | 16. ¬c<0
| . . . | ⊢  0≤(m ÷↓ p)  by SupposeNot
| . . . | |
| . . . | 1. p : ℤ^{-0}
| . . . | 2. prime(p)
| . . . | 3. 0<p
| . . . | 4. m : ℕ
| . . . | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . . | 6. n : ℕ
| . . . | 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . . | 8. ¬n = 0
| . . . | 9. m = (m ÷↓ p)·p+(m mod p)
| . . . | 10. (m mod p)<p
| . . . | 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . . | 12. p | ((m mod p)·(m mod p))
| . . . | 13. c : ℤ
| . . . | 14. (m mod p) = 0
| . . . | 15. c<1
| . . . | 16. ¬c<0
| . . . | 17. ¬0≤(m ÷↓ p)
| . . . | ⊢  0≤(m ÷↓ p)  by Assert ((m ÷↓ p)·p<0)
| . . . | |
| . . . | .....assertion .....
| . . . | 1. p : ℤ^{-0}
| . . . | 2. prime(p)
| . . . | 3. 0<p
| . . . | 4. m : ℕ
| . . . | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . . | 6. n : ℕ
| . . . | 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . . | 8. ¬n = 0
| . . . | 9. m = (m ÷↓ p)·p+(m mod p)
| . . . | 10. (m mod p)<p
| . . . | 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . . | 12. p | ((m mod p)·(m mod p))
| . . . | 13. c : ℤ
| . . . | 14. (m mod p) = 0
| . . . | 15. c<1
| . . . | 16. ¬c<0
| . . . | 17. ¬0≤(m ÷↓ p)
| . . . | ⊢  (m ÷↓ p)·p<0
| . . . |   by (RWO
| . . . |       Thm* ∀a,b:ℤ. a·b<0 ⟺ a<0 & b>0 ∨ a>0 & b<0
| . . . |       {neg_mul_arg_bounds}
| . . . |       0)
| . . . |      THEN
| . . . |      OrLeft
| . . . |
```

```
| . . . |\
| . . . | .....antecedent .....
| . . . | 1. p : ℤ⁻⁰
| . . . | 2. prime(p)
| . . . | 3. 0<p
| . . . | 4. m : ℕ
| . . . | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . . | 6. n : ℕ
| . . . | 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . . | 8. ¬n = 0
| . . . | 9. m = (m ÷↓ p)·p+(m mod p)
| . . . | 10. (m mod p)<p
| . . . | 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . . | 12. p | ((m mod p)·(m mod p))
| . . . | 13. c : ℤ
| . . . | 14. (m mod p) = 0
| . . . | 15. c<1
| . . . | 16. ¬c<0
| . . . | ⊢  n·n = p·(m ÷↓ p)·(m ÷↓ p)
| . . . | | by (HypSubst -3 7) THEN (ArithSimp 7)
| . . . | |
| . . . | 1. p : ℤ⁻⁰
| . . . | 2. prime(p)
| . . . | 3. 0<p
| . . . | 4. m : ℕ
| . . . | 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . . | 6. n : ℕ
| . . . | 7. p·p·(m ÷↓ p)·(m ÷↓ p) = n·n·p
| . . . | 8. ¬n = 0
| . . . | 9. m = (m ÷↓ p)·p+(m mod p)
| . . . | 10. (m mod p)<p
| . . . | 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . . | 12. p | ((m mod p)·(m mod p))
| . . . | 13. c : ℤ
| . . . | 14. (m mod p) = 0
| . . . | 15. c<1
| . . . | 16. ¬c<0
| . . . | ⊢  n·n = p·(m ÷↓ p)·(m ÷↓ p)
| . . . |   by Using [‘n’,p]
| . . . |      (BackThru
| . . . |       Thm* ∀a,b:ℤ, n:ℤ⁻⁰. n·a = n·b ⇒ a = b
| . . . |       {mul_cancel_in_eq})
| . . . |
| . . . .\
| . . . . 1. p : ℤ⁻⁰
| . . . . 2. prime(p)
| . . . . 3. 0<p
| . . . . 4. m : ℕ
| . . . . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . . . 6. n : ℕ
| . . . . 7. ((m ÷↓ p)·p+(m mod p))·((m ÷↓ p)·p+(m mod p)) = p·n·n
| . . . . 8. ¬n = 0
| . . . . 9. m = (m ÷↓ p)·p+(m mod p)
| . . . . 10. (m mod p)<p
| . . . . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
```

```
| . . . . . 12. p | ((m mod p)·(m mod p))
| . . . . . 13. c : ℤ
| . . . . . 14. (m mod p) = 0
| . . . . . 15. c<1
| . . . . . 16. ¬c<0
| . . . . . 17. (m ÷↓ p) = 0
| . . . . . ⊢  n = 0
| . . . . . | by (HypSubst -1 7) THEN (HypSubst -4 7)
| . . . . . |    THEN
| . . . . . |    (ArithSimp 7)
| . . . . . |
| . . . . . 1. p : ℤ⁻⁰
| . . . . . 2. prime(p)
| . . . . . 3. 0<p
| . . . . . 4. m : ℕ
| . . . . . 5. ∀m1:ℕ. m1<m ⇒ (∀n:ℕ. m1·m1 = p·n·n ⇒ n = 0)
| . . . . . 6. n : ℕ
| . . . . . 7. 0 = n·n·p
| . . . . . 8. ¬n = 0
| . . . . . 9. m = (m ÷↓ p)·p+(m mod p)
| . . . . . 10. (m mod p)<p
| . . . . . 11. ∀n@0:ℕ. n·n = p·n@0·n@0 ⇒ n@0 = 0
| . . . . . 12. p | ((m mod p)·(m mod p))
| . . . . . 13. c : ℤ
| . . . . . 14. (m mod p) = 0
| . . . . . 15. c<1
| . . . . . 16. ¬c<0
| . . . . . 17. (m ÷↓ p) = 0
| . . . . . ⊢  n = 0
| . . . .    by (Inst Thm* ∀a,b:ℕ+. 0<a·b    {mul_bounds_1b} [n;p])
| . . . .       THEN
| . . . .       (Inst Thm* ∀a,b:ℕ+. 0<a·b    {mul_bounds_1b} [n;n·p])
|
.\
. 1. p : ℤ⁻⁰
. 2. prime(p)
. 3. ¬0<p
. ⊢  ∀m,n:ℕ. m·m = p·n·n ⇒ n = 0  by Auto THEN SupposeNot
. |
. 1. p : ℤ⁻⁰
. 2. prime(p)
. 3. ¬0<p
. 4. m : ℕ
. 5. n : ℕ
. 6. m·m = p·n·n
. 7. ¬n = 0
. ⊢  n = 0  by Assert (p·n·n<0)
. |
. |\
. | .....assertion .....
. | 1. p : ℤ⁻⁰
. | 2. prime(p)
. | 3. ¬0<p
. | 4. m : ℕ
. | 5. n : ℕ
```

```
. | 6. m·m = p·n·n
. | 7. ¬n = 0
. | ⊢  p·n·n<0
. | | by (RWO
. | |     Thm* ∀a,b:ℤ. a·b<0 ⟺ a<0 & b>0 ∨ a>0 & b<0
. | |     {neg_mul_arg_bounds}
. | |     0)
. | |    THEN
. | |    OrLeft
. | |
. | 1. p : ℤ⁻⁰
. | 2. prime(p)
. | 3. ¬0<p
. | 4. m : ℕ
. | 5. n : ℕ
. | 6. m·m = p·n·n
. | 7. ¬n = 0
. | ⊢  n·n>0
. |   by (RWO
. |       Thm* ∀a,b:ℤ. a·b>0 ⟺ a>0 & b>0 ∨ a<0 & b<0
. |       {pos_mul_arg_bounds}
. |       0)
. |      THEN
. |      OrLeft
. |
. .\
. . 1. p : ℤ⁻⁰
. . 2. prime(p)
. . 3. ¬0<p
. . 4. m : ℕ
. . 5. n : ℕ
. . 6. m·m = p·n·n
. . 7. ¬n = 0
. . 8. p·n·n<0
. . ⊢  n = 0  by Assert (0≤m·m)
. . |
. . .....assertion .....
. . 1. p : ℤ⁻⁰
. . 2. prime(p)
. . 3. ¬0<p
. . 4. m : ℕ
. . 5. n : ℕ

. . 6. m·m = p·n·n
. . 7. ¬n = 0
. . 8. p·n·n<0
. . ⊢  0≤m·m  by BackThru Thm* ∀a,b:ℕ. 0≤a·b    {mul_bounds_1a}
END
```