```
primes_sqr_roots_LEMMA1  THM

⊢  ∀a:ℕ.
|  prime(a)
|  ⇒
|  (∀p:ℕ, q:ℕ+. p·p = a·q·q ⇒ (∃p':ℕ+. p'<p & q·q = a·p'·p'))
| by Auto
|
1. a : ℕ
2. prime(a)
3. p : ℕ
4. q : ℕ+
5. p·p = a·q·q
⊢  ∃p':ℕ+. p'<p & q·q = a·p'·p'
| by FwdThru:
|     Thm*  ∀a:ℤ. prime(a) ⇒ (∀x:ℤ. a | x·x ⟺ a | x)
|     {prime_divides_square}
|     on [ a | p·p ]
|
|\
| .....assertion .....
| ⊢  a | p·p  by Witness: q·q
|
.\
. 6. a | p
. ⊢  ∃p':ℕ+. p'<p & q·q = a·p'·p'  by New:p' Analyze6
. |
. 6. p' : ℤ
. 7. p = a·p'
. ⊢  ∃p':ℕ+. p'<p & q·q = a·p'·p'
. | by a>0 & p>0 & p'>0  By SideProof 1
. |
. 8. a>0
. 9. p>0
. 10. p'>0
. ⊢  ∃p':ℕ+. p'<p & q·q = a·p'·p'  by Witness: p'
. |
. |\
. | ⊢  p'<p
. | | by Use:[n:= a]
. | |    BackThru:
. | |    Thm*  ∀a,b:ℤ, n:ℕ+. n·a<n·b ⇒ a<b    {mul_cancel_in_lt}
. | |
. | ⊢  a·p'<a·p  by Rewrite by 1·p = a·p' {← hyp Hyp:7 }
. | |
. | ⊢  1·p<a·p  by Rewrite by Thm*  ∀a,b:ℤ. a·b = b·a    {mul_com}
. | |
. | ⊢  p·1<p·a
. | | by BackThru:
. | |    Thm*  ∀a,b:ℤ, n:ℕ+. a<b ⇒ n·a<n·b    {mul_preserves_lt}
. | |
. | ⊢  1<a
. |   by FwdThru:
. |      Thm*  ∀x:ℕ. prime(x) ⟺ 2≤x & ¬(∃i:{2..x⁻}. i | x)
. |      {prime_nat}
```

```
. |      on [ prime(a) ]
. |
. .\
. . ⊢  q·q = a·p'·p'  by Use:[n:= a] BackThru: Thm: mul_cancel_in_eq
. . |
. . ⊢  a·q·q = a·a·p'·p'
. .   by Rewrite by a·a·p'·p' = a·p'·a·p' {← hyps Hyp:5 Hyp:7 }
END
---
primes_sqr_roots_LEMMA1 Side Proof 1  THM

.....assertion .....
1. a : ℕ
2. prime(a)
3. p : ℕ
4. q : ℕ+
5. p·p = a·q·q
6. p' : ℤ
7. p = a·p'
⊢  a>0 & p>0 & p'>0
| by ∀a:ℕ, b:ℤ. a·b>0 ⟺ a>0 & b>0
|      By SimilarTo: Thm: pos_mul_arg_bounds
|
8. ∀a:ℕ, b:ℤ. a·b>0 ⟺ a>0 & b>0
⊢  a>0 & p>0 & p'>0
  by a>0  By Analyze2 THEN a·q·q>0  By Repeat BackThru: Hyp:8
     THEN
     p>0  By FwdThru: Hyp:8 on [ p·p>0 ]
     THEN
     p'>0  By Sel 2 FwdThru: Hyp:8 on [ a·p'>0 ]
END
```