```
can_reduce_composite_factor  THM

⊢  ∀k:{2...}, g:({2..k⁻}→ℕ), x,y:{2..k⁻}.
|  x·y<k
|  ⇒
|  (∃h:({2..k⁻}→ℕ).
|   Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
|   & h(x·y) = 0
|   & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u)))
| by Guarding (∀x:<type>. <prop>) Autoℕ
|
1. k : {2...}
2. g : {2..k⁻}→ℕ
⊢  ∀x,y:{2..k⁻}.
|  x·y<k
|  ⇒
|  (∃h:({2..k⁻}→ℕ).
|   Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
|   & h(x·y) = 0
|   & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u)))
| by {Without loss of generality, assume x≤y and observe that y<x·y
|     (hence x·y ∈ {2..k⁻})
|     }
|    SideProof 1
|
3. x : {2..k⁻}
4. y : {2..k⁻}
5. x≤y
6. x·y<k
7. y<x·y
⊢  ∃h:({2..k⁻}→ℕ).
|  Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
|  & h(x·y) = 0
|  & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u))  by Decide: x<y ...wℕ
|
|\
| 8. x<y
| ⊢  ∃h:({2..k⁻}→ℕ).
| |  Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
| |  & h(x·y) = 0
| |  & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u))
| | by Witness: split_factor2(g; x; y) ...wℕ
| |
| ⊢  Π↑{2..k⁻}(g) = Π↑{2..k⁻}(split_factor2(g; x; y))
|    & split_factor2(g; x; y)(x·y) = 0
|    & (∀u:{2..k⁻}. x·y<u ⇒ split_factor2(g; x; y)(u) = g(u))
|   by Guarding (<prop> & <prop>)
|      BackThru:
|      Thm*  ∀k:{2...}, g:({2..k⁻}→ℕ), x,y:{2..k⁻}.
|            x·y<k
|            ⇒
|            x<y
|            ⇒
|            Π↑{2..k⁻}(g) = Π↑{2..k⁻}(split_factor2(g; x; y))
|            & split_factor2(g; x; y)(x·y) = 0
```

```
|             & (∀u:{2..k⁻}. x·y<u ⇒ split_factor2(g; x; y)(u) = g(u))
|      {split_factor2_char} ...ℕ
|
.\
. 8. ¬x<y
. ⊢  ∃h:({2..k⁻}→ℕ).
. |  Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
. |  & h(x·y) = 0
. |  & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u))
. | by Rewrite by x·y = x·x ∈ {2..k⁻} ...aℕ
. |
. ⊢  ∃h:({2..k⁻}→ℕ).
. |  Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
. |  & h(x·x) = 0
. |  & (∀u:{2..k⁻}. x·x<u ⇒ h(u) = g(u))
. | by Witness: split_factor1(g; x)
. |
. ⊢  Π↑{2..k⁻}(g) = Π↑{2..k⁻}(split_factor1(g; x))
.    & split_factor1(g; x)(x·x) = 0
.    & (∀u:{2..k⁻}. x·x<u ⇒ split_factor1(g; x)(u) = g(u))
.   by Guarding (<prop> & <prop>)
.      BackThru:
.      Thm*  ∀k:{2...}, g:({2..k⁻}→ℕ), x:{2..k⁻}.
.             x·x<k
.             ⇒
.             Π↑{2..k⁻}(g) = Π↑{2..k⁻}(split_factor1(g; x))
.             & split_factor1(g; x)(x·x) = 0
.             & (∀u:{2..k⁻}. x·x<u ⇒ split_factor1(g; x)(u) = g(u))
.      {split_factor1_char}
END
---

can_reduce_composite_factor Side Proof 1  THM

1. k : {2...}
2. g : {2..k⁻}→ℕ
⊢  ∀x,y:{2..k⁻}.
|  x·y<k
|  ⇒
|  (∃h:({2..k⁻}→ℕ).
|   Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
|   & h(x·y) = 0
|   & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u)))
| by ∀x,y:{2..k⁻}.
|    x≤y
|    ⇒
|    x·y<k
|    ⇒
|    (∃h:({2..k⁻}→ℕ).
|     Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
|     & h(x·y) = 0
|     & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u)))
|    Asserted ...ℕ
|    THEN
|    Inst: Thm*  ∀i:{2...}, j:{1...}. j<i·j    {factor_smaller}
```

```
|    Using:[x | y] ...wℕ
|
|\
| 3. x : {2..k⁻}
| 4. y : {2..k⁻}
| 5. x≤y
| 6. x·y<k
| 7. y<x·y
| ⊢  ∃h:({2..k⁻}→ℕ).
|    Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
|    & h(x·y) = 0
|    & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u))  by <Unproved PREMISE>
|
.\
. 3. ∀x,y:{2..k⁻}.
. |  x≤y
. |  ⇒
. |  x·y<k
. |  ⇒
. |  (∃h:({2..k⁻}→ℕ).
. |   Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
. |   & h(x·y) = 0
. |   & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u)))
. 4. x : {2..k⁻}
. 5. y : {2..k⁻}
. 6. x·y<k
. 7. y<x·y
. ⊢  ∃h:({2..k⁻}→ℕ).
. |  Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
. |  & h(x·y) = 0
. |  & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u))
. | by Decide: x≤y ...wℕ
. |    THENL
. |    [Inst: Hyp:3 Using:[x | y] ...ℕ
. |    ;Inst: Hyp:3 Using:[y | x] ...ℕ]
. |
. 8. ¬x≤y
. 9. ∃h:({2..k⁻}→ℕ).
.    Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
.    & h(y·x) = 0
.    & (∀u:{2..k⁻}. y·x<u ⇒ h(u) = g(u))
. ⊢  ∃h:({2..k⁻}→ℕ).
.    Π↑{2..k⁻}(g) = Π↑{2..k⁻}(h)
.    & h(x·y) = 0
.    & (∀u:{2..k⁻}. x·y<u ⇒ h(u) = g(u))  by SimilarTo: Hyp:-1 ...ℕ
END
```