```
bezout_ident_n_sfa  THM

⊢  ∀b:ℕ, a:ℤ. ∃u,v:ℤ. GCD(a;b;u•a+v•b)  by CompNatInd Concl
|
1. b : ℕ
2. ∀b⁻:ℕ. b⁻<b ⇒ (∀a:ℤ. ∃u,v:ℤ. GCD(a;b⁻;u•a+v•b⁻))
⊢  ∀a:ℤ. ∃u,v:ℤ. GCD(a;b;u•a+v•b)
| by Specialize inductive hyp with b for a
|
2. ∀b⁻:ℕ. b⁻<b ⇒ (∃u,v:ℤ. GCD(b;b⁻;u•b+v•b⁻))
3. a : ℤ
⊢  ∃u,v:ℤ. GCD(a;b;u•a+v•b)  by Decide: b = 0
|
|\
| 4. b = 0
| ⊢  ∃u,v:ℤ. GCD(a;b;u•a+v•b)  by Witness: 1 | 0
| |
| ⊢  GCD(a;b;1•a+0•b)  by Thm* ∀a:ℤ. GCD(a;0;a)    {gcd_p_zero}
|
.\
. 4. ¬b = 0
. ⊢  ∃u,v:ℤ. GCD(a;b;u•a+v•b)
. | by Make the goal match the conclusion of Hyp:2, using
. |    Thm* ∀a,b,y:ℤ. GCD(a;b;y) ⇒ GCD(b;a;y)    {gcd_p_sym} and
. |    Thm* ∀a,b:ℤ. a+b = b+a    {add_com}
. |
. ⊢  ∃u,v:ℤ. GCD(b;a;u•b+v•a)
. | by Inst:
. |    Thm* ∀a:ℤ, b:ℕ⁺. ∃q:ℤ, r:ℕb. a = q•b+r    {quot_rem_exists}
. |    Using:[a | b]
. |    THEN
. |    ExistHD Hyp:-1 THEN Rewrite by a = r+q•b
. |
. 5. q : ℤ
. 6. r : ℕb
. 7. a = q•b+r
. ⊢  ∃u,v:ℤ. GCD(b;r+q•b;u•b+v•(r+q•b))  by FwdThru: Hyp:2 on [ r<b ]
. |
. 8. ∃x,y:ℤ. GCD(b;r;x•b+y•r)
. ⊢  ∃u,v:ℤ. GCD(b;r+q•b;u•b+v•(r+q•b))
. | by Thm* ∀a,b,y,k:ℤ. GCD(a;b;y) ⇒ GCD(a;b+k•a;y)    {gcd_p_shift}
. |
. 8. ∃x,y:ℤ. GCD(b;r+q•b;x•b+y•r)
. ⊢  ∃u,v:ℤ. GCD(b;r+q•b;u•b+v•(r+q•b))  by ExistHD Hyp:-1
. |
. 8. x : ℤ
. 9. y : ℤ
. 10. GCD(b;r+q•b;x•b+y•r)
. ⊢  ∃u,v:ℤ. GCD(b;r+q•b;u•b+v•(r+q•b))
. | by Last hyp and goal match except in one argument place.
. |
. ⊢  ∃u,v:ℤ. u•b+v•(r+q•b) = x•b+y•r  by using y for v
. |
. ⊢  ∃u:ℤ. u•b+y•(r+q•b) = x•b+y•r  by r drops out
. |
```

```
. ⊢  ∃u:ℤ. u·b+y·q·b = x·b  by b drops out
. |
. ⊢  ∃u:ℤ. u+y·q = x  by Witness: x-y·q
END
```