```
chrem_exists_a  THM

⊢  ∀r:ℕ+, s:{s':ℕ+| CoPrime(r,s') }, a,b:ℤ.
|  ↓∃x:ℤ. ((x = a mod r) & (x = b mod s))  by UnivCD
|
1. r : ℕ+
2. s : {s':ℕ+| CoPrime(r,s') }
3. a : ℤ
4. b : ℤ
⊢  ↓∃x:ℤ. ((x = a mod r) & (x = b mod s))
| by Analyze 2 THEN UnhideSqStableHyp 3
|
2. s : ℕ+
3. CoPrime(r,s)
4. a : ℤ
5. b : ℤ
⊢  ↓∃x:ℤ. ((x = a mod r) & (x = b mod s))
| by (Inst
|     Thm* ∀r:ℕ+, s:{s':ℕ+| CoPrime(r,s') }.
|           ↓∃x:ℤ. ((x = 1 mod r) & (x = 0 mod s))
|     {chrem_exists_aux_a}
|     [r;s])
|    THEN
|    (Inst
|     Thm* ∀r:ℕ+, s:{s':ℕ+| CoPrime(r,s') }.
|           ↓∃x:ℤ. ((x = 1 mod r) & (x = 0 mod s))
|     {chrem_exists_aux_a}
|     [s;r])
|
|\
| .....set predicate .....
| 6. ↓∃x:ℤ. ((x = 1 mod r) & (x = 0 mod s))
| ⊢  CoPrime(s,r)  by OnClauses [3;0] UnfoldTopAb
| |
| 3. GCD(r;s;1)
| 4. ℤ
| 5. ℤ
| 6. ↓∃x:ℤ. ((x = 1 mod r) & (x = 0 mod s))
| ⊢  GCD(s;r;1)
|   by BackThru
|      Thm* ∀a,b,y:ℤ. GCD(a;b;y) ⇒ GCD(b;a;y)    {gcd_p_sym}
|
.\
. 6. ↓∃x:ℤ. ((x = 1 mod r) & (x = 0 mod s))
. 7. ↓∃x:ℤ. ((x = 1 mod s) & (x = 0 mod r))
. ⊢  ↓∃x:ℤ. ((x = a mod r) & (x = b mod s))
. | by New ['q'] (Analyze 7) THEN New ['p'] (Analyze 6)
. |
. 6. p : ℤ
. 7. (p = 1 mod r) & (p = 0 mod s)  [not for witness]
. 8. q : ℤ
. 9. (q = 1 mod s) & (q = 0 mod r)  [not for witness]
. ⊢  ↓∃x:ℤ. ((x = a mod r) & (x = b mod s))
. | by SeqOnM [Witness a·p+b·q;Analyze 9;Analyze 7;Analyze 0]
. |
```

```
. |\
. | 7. p = 1 mod r
. | 8. p = 0 mod s
. | 9. q : ℤ
. | 10. q = 1 mod s
. | 11. q = 0 mod r
. | ⊢  (a·p+b·q) = a mod r
. | | by (RewriteWith [7;11] [] 0) THEN (ArithSimp 0)
. | |
. | ⊢  a = a mod r
. |   by BackThru
. |      Thm* ∀m,a,b:ℤ. a = b ⇒ (a = b mod m)    {eqmod_weakening}
. |
. .\
. . 7. p = 1 mod r
. . 8. p = 0 mod s
. . 9. q : ℤ
. . 10. q = 1 mod s
. . 11. q = 0 mod r
. . ⊢  (a·p+b·q) = b mod s
. . | by (RewriteWith [8;10] [] 0) THEN (ArithSimp 0)
. . |
. . ⊢  b = b mod s
. .   by BackThru
. .      Thm* ∀m,a,b:ℤ. a = b ⇒ (a = b mod m)    {eqmod_weakening}
END
```