```
chrem_exists  THM

⊢  ∀r,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 : 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,s:ℕ⁺.
|          CoPrime(r,s) ⇒ (∃x:ℤ. (x = 1 mod r) & (x = 0 mod s))
|     {chrem_exists_aux}
|     [r;s])
|    THEN
|    (Inst
|     Thm* ∀r,s:ℕ⁺.
|          CoPrime(r,s) ⇒ (∃x:ℤ. (x = 1 mod r) & (x = 0 mod s))
|     {chrem_exists_aux}
|     [s;r])
|
|\
| .....antecedent .....
| 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)
. |    THEN
. |    TryOnAllHyps ExistHD
. |
. 6. p : ℤ
. 7. p = 1 mod r
. 8. p = 0 mod s
. 9. q : ℤ
. 10. q = 1 mod s
. 11. q = 0 mod r
. ⊢  ∃x:ℤ. (x = a mod r) & (x = b mod s)
. | by Witness a·p+b·q THEN (Analyze 0)
. |
. |\
```

```
. | ⊢  (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}
. |
. .\
. . ⊢  (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
```