```
⊢ ∀m:ℤ. ∀n:ℤ⁻⁰. ∀g:ℤ.  (GCD(m;n;g) ⟺ GCD(n;m rem n;g))
|
BY RepeatFor 3 ((D 0 THENA Auto))
|
1. m: ℤ
2. n: ℤ⁻⁰
3. g: ℤ
⊢ GCD(m;n;g) ⟺ GCD(n;m rem n;g)
|
BY D 0
|\
| ⊢ GCD(m;n;g) ⇒ GCD(n;m rem n;g)
| |
1 BY (D 0 THENA Auto)
| |
| 4. GCD(m;n;g)
| ⊢ GCD(n;m rem n;g)
| |
1 BY All(Unfold `gcd_p`)
| |
| 4. (g | m) ∧ (g | n) ∧ (∀z:ℤ. (((z | m) ∧ (z | n)) ⇒ (z | g)))
| ⊢ (g | n) ∧ (g | (m rem n)) ∧ (∀z:ℤ. (((z | n) ∧ (z | (m rem n))) ⇒ (z | g)))
| |
1 BY D 4
| |
| 4. g | m
| 5. (g | n) ∧ (∀z:ℤ. (((z | m) ∧ (z | n)) ⇒ (z | g)))
| ⊢ (g | n) ∧ (g | (m rem n)) ∧ (∀z:ℤ. (((z | n) ∧ (z | (m rem n))) ⇒ (z | g)))
| |
1 BY D 5
| |
| 5. g | n
| 6. ∀z:ℤ. (((z | m) ∧ (z | n)) ⇒ (z | g))
| ⊢ (g | n) ∧ (g | (m rem n)) ∧ (∀z:ℤ. (((z | n) ∧ (z | (m rem n))) ⇒ (z | g)))
| |
1 BY D 0
| |\
| | ⊢ g | n
| | |
1 2 BY NthHyp 5
|  \
|   ⊢ (g | (m rem n)) ∧ (∀z:ℤ. (((z | n) ∧ (z | (m rem n))) ⇒ (z | g)))
|   |
1   BY D 0
|   |\
|   | ⊢ g | (m rem n)
|   | |
1   2 BY All(Unfold `divides`)
|   | |
|   | 4. ∃c:ℤ. (m = (g * c))
|   | 5. ∃c:ℤ. (n = (g * c))
|   | 6. ∀z:ℤ. (((∃c:ℤ. (m = (z * c))) ∧ (∃c:ℤ. (n = (z * c)))) ⇒ (∃c:ℤ. (g = (z * c))))
|   | ⊢ ∃c:ℤ. ((m rem n) = (g * c))
```

```
|   | |
1   2 BY D 4
|   | |
|   | 4. c: ℤ
|   | 5. m = (g * c)
|   | 6. ∃c:ℤ. (n = (g * c))
|   | 7. ∀z:ℤ. (((∃c:ℤ. (m = (z * c))) ∧ (∃c:ℤ. (n = (z * c)))) ⇒ (∃c:ℤ. (g = (z * c))))
|   | ⊢ ∃c:ℤ. ((m rem n) = (g * c))
|   | |
1   2 BY D 6
|   | |
|   | 6. c1: ℤ
|   | 7. n = (g * c1)
|   | 8. ∀z:ℤ. (((∃c:ℤ. (m = (z * c))) ∧ (∃c:ℤ. (n = (z * c)))) ⇒ (∃c:ℤ. (g = (z * c))))
|   | ⊢ ∃c:ℤ. ((m rem n) = (g * c))
|   | |
1   2 BY (InstLemma ‘rem_to_div‘ [⌈m⌉;⌈n⌉]· THENA Auto)
|   | |
|   | 9. (m rem n) = (m - (m ÷ n) * n)
|   | ⊢ ∃c:ℤ. ((m rem n) = (g * c))
|   | |
1   2 BY Assert ⌈(m rem n) = ((g * c) - (m ÷ n) * g * c1)⌉·
|   | |\
|   | | ⊢ (m rem n) = ((g * c) - (m ÷ n) * g * c1)
|   | | |
1   2 3 BY Auto’
|   |  \
|   |   10. (m rem n) = ((g * c) - (m ÷ n) * g * c1)
|   |   ⊢ ∃c:ℤ. ((m rem n) = (g * c))
|   |   |
1   2   BY (InstConcl [⌈c - (m ÷ n) * c1⌉]· THENA Auto)
|   |   |
|   |   ⊢ (m rem n) = (g * (c - (m ÷ n) * c1))
|   |   |
1   2   BY Auto’
|    \
|     ⊢ ∀z:ℤ. (((z | n) ∧ (z | (m rem n))) ⇒ (z | g))
|     |
1     BY RepeatFor 2 ((D 0 THENA Auto))
|     |
|     7. z: ℤ
|     8. (z | n) ∧ (z | (m rem n))
|     ⊢ z | g
|     |
1     BY D 8
|     |
|     8. z | n
|     9. z | (m rem n)
|     ⊢ z | g
|     |
1     BY (SimpleInstHyp ⌈z⌉ 6· THENA Auto)
|     |
|     10. ((z | m) ∧ (z | n)) ⇒ (z | g)
|     ⊢ z | g
```

```
|     |
1     BY D 10
|     |\
|     | ⊢ (z | m) ∧ (z | n)
|     | |
1     2 BY D 0
|     | |\
|     | | ⊢ z | m
|     | | |
1     2 3 BY All(Unfold ‘divides‘)
|     | | |
|     | | 4. ∃c:ℤ. (m = (g * c))
|     | | 5. ∃c:ℤ. (n = (g * c))
|     | | 6. ∀z:ℤ. (((∃c:ℤ. (m = (z * c))) ∧ (∃c:ℤ. (n = (z * c)))) ⇒ (∃c:ℤ. (g = (z * c))))
|     | | 8. ∃c:ℤ. (n = (z * c))
|     | | 9. ∃c:ℤ. ((m rem n) = (z * c))
|     | | ⊢ ∃c:ℤ. (m = (z * c))
|     | | |
1     2 3 BY D 8
|     | | |
|     | | 8. c: ℤ
|     | | 9. n = (z * c)
|     | | 10. ∃c:ℤ. ((m rem n) = (z * c))
|     | | ⊢ ∃c:ℤ. (m = (z * c))
|     | | |
1     2 3 BY D 10
|     | | |
|     | | 10. c1: ℤ
|     | | 11. (m rem n) = (z * c1)
|     | | ⊢ ∃c:ℤ. (m = (z * c))
|     | | |
1     2 3 BY (InstLemma ‘div_rem_sum‘ [⌈m⌉;⌈n⌉]· THENA Auto)
|     | | |
|     | | 12. m = (((m ÷ n) * n) + (m rem n))
|     | | ⊢ ∃c:ℤ. (m = (z * c))
|     | | |
1     2 3 BY Assert ⌈m = (((m ÷ n) * z * c) + (z * c1))⌉·
|     | | |\
|     | | | ⊢ m = (((m ÷ n) * z * c) + (z * c1))
|     | | | |
1     2 3 4 BY Auto’
|     | |  \
|     | |   13. m = (((m ÷ n) * z * c) + (z * c1))
|     | |   ⊢ ∃c:ℤ. (m = (z * c))
|     | |   |
1     2 3   BY (InstConcl [⌈((m ÷ n) * c) + c1⌉]· THENA Auto)
|     | |   |
|     | |   ⊢ m = (z * (((m ÷ n) * c) + c1))
|     | |   |
1     2 3   BY Auto’
|     |  \
|     |   ⊢ z | n
|     |   |
1     2   BY NthHyp 8
```

```
|      \
|       10. z | g
|       ⊢ z | g
|       |
1       BY NthHyp 10
 \
  ⊢ GCD(m;n;g) ⇐ GCD(n;m rem n;g)
  |
  BY (D 0 THENA Auto)
  |
  4. GCD(n;m rem n;g)
  ⊢ GCD(m;n;g)
  |
  BY All(Unfold `gcd_p`)·
  |
  4. (g | n) ∧ (g | (m rem n)) ∧ (∀z:ℤ. (((z | n) ∧ (z | (m rem n))) ⇒ (z | g)))
  ⊢ (g | m) ∧ (g | n) ∧ (∀z:ℤ. (((z | m) ∧ (z | n)) ⇒ (z | g)))
  |
  BY D 4
  |
  4. g | n
  5. (g | (m rem n)) ∧ (∀z:ℤ. (((z | n) ∧ (z | (m rem n))) ⇒ (z | g)))
  ⊢ (g | m) ∧ (g | n) ∧ (∀z:ℤ. (((z | m) ∧ (z | n)) ⇒ (z | g)))
  |
  BY D 5
  |
  5. g | (m rem n)
  6. ∀z:ℤ. (((z | n) ∧ (z | (m rem n))) ⇒ (z | g))
  ⊢ (g | m) ∧ (g | n) ∧ (∀z:ℤ. (((z | m) ∧ (z | n)) ⇒ (z | g)))
  |
  BY D 0
  |\
  | ⊢ g | m
  | |
  1 BY All(Unfold `divides`)
  | |
  | 4. ∃c:ℤ. (n = (g * c))
  | 5. ∃c:ℤ. ((m rem n) = (g * c))
  | 6. ∀z:ℤ. (((∃c:ℤ. (n = (z * c))) ∧ (∃c:ℤ. ((m rem n) = (z * c)))) ⇒ (∃c:ℤ. (g = (z * c))))
  | ⊢ ∃c:ℤ. (m = (g * c))
  | |
  1 BY D 4
  | |
  | 4. c: ℤ
  | 5. n = (g * c)
  | 6. ∃c:ℤ. ((m rem n) = (g * c))
  | 7. ∀z:ℤ. (((∃c:ℤ. (n = (z * c))) ∧ (∃c:ℤ. ((m rem n) = (z * c)))) ⇒ (∃c:ℤ. (g = (z * c))))
  | ⊢ ∃c:ℤ. (m = (g * c))
  | |
  1 BY D 6
  | |
  | 6. c1: ℤ
  | 7. (m rem n) = (g * c1)
  | 8. ∀z:ℤ. (((∃c:ℤ. (n = (z * c))) ∧ (∃c:ℤ. ((m rem n) = (z * c)))) ⇒ (∃c:ℤ. (g = (z * c))))
```

```
| ⊢ ∃c:ℤ. (m = (g * c))
| |
1 BY (InstLemma 'div_rem_sum' [⌈m⌉;⌈n⌉]· THENA Auto)
| |
| 9. m = (((m ÷ n) * n) + (m rem n))
| ⊢ ∃c:ℤ. (m = (g * c))
| |
1 BY Assert ⌈m = (((m ÷ n) * g * c) + (g * c1))⌉·
| |\
| | ⊢ m = (((m ÷ n) * g * c) + (g * c1))
| | |
1 2 BY Auto'
|  \
|   10. m = (((m ÷ n) * g * c) + (g * c1))
|   ⊢ ∃c:ℤ. (m = (g * c))
|   |
1   BY (InstConcl [⌈((m ÷ n) * c) + c1⌉]· THENA Auto)
|   |
|   ⊢ m = (g * (((m ÷ n) * c) + c1))
|   |
1   BY Auto'
 \
  ⊢ (g | n) ∧ (∀z:ℤ. (((z | m) ∧ (z | n)) ⇒ (z | g)))
  |
  BY D 0
  |\
  | ⊢ g | n
  | |
  1 BY NthHyp 4
   \
    ⊢ ∀z:ℤ. (((z | m) ∧ (z | n)) ⇒ (z | g))
    |
    BY RepeatFor 2 ((D 0 THENA Auto))
    |
    7. z: ℤ
    8. (z | m) ∧ (z | n)
    ⊢ z | g
    |
    BY D 8
    |
    8. z | m
    9. z | n
    ⊢ z | g
    |
    BY (SimpleInstHyp ⌈z⌉ 6· THENA Auto)
    |
    10. ((z | n) ∧ (z | (m rem n))) ⇒ (z | g)
    ⊢ z | g
    |
    BY D 10
    |\
    | ⊢ (z | n) ∧ (z | (m rem n))
    | |
    1 BY D 0
```

```
| |\
| | ⊢ z | n
| | |
1 2 BY NthHyp 9
|  \
|   ⊢ z | (m rem n)
|   |
1   BY All(Unfold ‘divides‘)
|   |
|   4. ∃c:ℤ. (n = (g * c))
|   5. ∃c:ℤ. ((m rem n) = (g * c))
|   6. ∀z:ℤ
|        (((∃c:ℤ. (n = (z * c))) ∧ (∃c:ℤ. ((m rem n) = (z * c)))) ⇒ (∃c:ℤ. (g = (z * c))))
|   8. ∃c:ℤ. (m = (z * c))
|   9. ∃c:ℤ. (n = (z * c))
|   ⊢ ∃c:ℤ. ((m rem n) = (z * c))
|   |
1   BY D 8
|   |
|   8. c: ℤ
|   9. m = (z * c)
|   10. ∃c:ℤ. (n = (z * c))
|   ⊢ ∃c:ℤ. ((m rem n) = (z * c))
|   |
1   BY D 10
|   |
|   10. c1: ℤ
|   11. n = (z * c1)
|   ⊢ ∃c:ℤ. ((m rem n) = (z * c))
|   |
1   BY (InstLemma ‘rem_to_div‘ [⌈m⌉;⌈n⌉]⋅ THENA Auto)
|   |
|   12. (m rem n) = (m - (m ÷ n) * n)
|   ⊢ ∃c:ℤ. ((m rem n) = (z * c))
|   |
1   BY Assert ⌈(m rem n) = ((z * c) - (m ÷ n) * z * c1)⌉⋅
|   |\
|   | ⊢ (m rem n) = ((z * c) - (m ÷ n) * z * c1)
|   | |
1   2 BY Auto’
|    \
|     13. (m rem n) = ((z * c) - (m ÷ n) * z * c1)
|     ⊢ ∃c:ℤ. ((m rem n) = (z * c))
|     |
1     BY (InstConcl [⌈c - (m ÷ n) * c1⌉]⋅ THENA Auto)
|     |
|     ⊢ (m rem n) = (z * (c - (m ÷ n) * c1))
|     |
1     BY Auto’
 \
  10. z | g
  ⊢ z | g
  |
  BY NthHyp 10
```