Extended Euclid's Algorithm

Extended Euclid's Algorithm

Example 67

$$
\begin{array}{rl}
 & \gcd(34,13) \\
= & \gcd(13,8) \\
= & \gcd(8,5) \\
= & \gcd(5,3) \\
= & \gcd(3,2) \\
= & \gcd(2,1) \\
= & 1
\end{array}
\qquad
\left\|\begin{array}{rcrcl}
34 & = & 2\cdot & 13 & +\ 8 \\
13 & = & 1\cdot & 8 & +\ 5 \\
8 & = & 1\cdot & 5 & +\ 3 \\
5 & = & 1\cdot & 3 & +\ 2 \\
3 & = & 1\cdot & 2 & +\ 1 \\
2 & = & 2\cdot & 1 & +\ 0
\end{array}\right\|
$$

Extended Euclid's Algorithm

Example 67

$$
\begin{array}{rl}
 & \gcd(34,13) \\
= & \gcd(13,8) \\
= & \gcd(8,5) \\
= & \gcd(5,3) \\
= & \gcd(3,2) \\
= & \gcd(2,1) \\
= & 1
\end{array}
\qquad
\begin{array}{rcrcl}
34 & = & 2\cdot & 13 & +\ 8 \\
13 & = & 1\cdot & 8 & +\ 5 \\
8 & = & 1\cdot & 5 & +\ 3 \\
5 & = & 1\cdot & 3 & +\ 2 \\
3 & = & 1\cdot & 2 & +\ 1 \\
2 & = & 2\cdot & 1 & +\ 0
\end{array}
\qquad
\begin{array}{rcrcl}
8 & = & 34 & -2\cdot & 13 \\
5 & = & 13 & -1\cdot & 8 \\
3 & = & 8 & -1\cdot & 5 \\
2 & = & 5 & -1\cdot & 3 \\
1 & = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{rl||rrrr}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & & & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & & & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & & & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{rl||rrrr}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)}^{8} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & & & & \\
 & & & & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & & & & \\
 & & & & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{lll||rcrcl}
 & \gcd(34,13) & 8 & = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)}^{8} \\
 & & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)}^{8} \\
 & & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 & = & \overbrace{(34-2\cdot 13)}^{8} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)}^{5} \\
 & & & = & \overbrace{(34-2\cdot 13)}^{8} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)}^{5} \\
 & & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 & = & 5 & -1\cdot & 3 \\
 & & & & & & \\
 & & & & & & \\
= & \gcd(3,2) & 1 & = & 3 & -1\cdot & 2 \\
 & & & & & & \\
 & & & & & &
\end{array}
$$

$$
\begin{array}{rl||rcrcl}
 & \gcd(34,13) & 8 & = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)}^{8} \\
 & & & = & 13 & -1\cdot & (34-2\cdot 13) \\
 & & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 & = & \overbrace{(34-2\cdot 13)}^{8} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)}^{5} \\
 & & & = & (34-2\cdot 13) & -1\cdot & (-1\cdot 34+3\cdot 13) \\
 & & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 & = & \overbrace{-1\cdot 34+3\cdot 13}^{5} & -1\cdot & \overbrace{(2\cdot 34+(-5)\cdot 13)}^{3} \\
 & & & = & -1\cdot 34+3\cdot 13 & -1\cdot & (2\cdot 34+(-5)\cdot 13) \\
 & & & = & -3\cdot 34+8\cdot 13 & & \\
= & \gcd(3,2) & 1 & = & 3 & -1\cdot & 2
\end{array}
$$

NB : gcd(34,13) is an integer linear combination of 34 and 13.

$$
\begin{aligned}
& \gcd(34,13) && 8 = 34 - 2\cdot 13 \\
= \ & \gcd(13,8) && 5 = 13 - 1\cdot 8 \\
& && \quad = 13 - 1\cdot(34 - 2\cdot 13) \\
& && \quad = -1\cdot 34 + 3\cdot 13 \\
= \ & \gcd(8,5) && 3 = 8 - 1\cdot 5 \\
& && \quad = (34 - 2\cdot 13) - 1\cdot(-1\cdot 34 + 3\cdot 13) \\
& && \quad = 2\cdot 34 + (-5)\cdot 13 \\
= \ & \gcd(5,3) && 2 = 5 - 1\cdot 3 \\
& && \quad = (-1\cdot 34 + 3\cdot 13) - 1\cdot(2\cdot 34 + (-5)\cdot 13) \\
& && \quad = -3\cdot 34 + 8\cdot 13 \\
= \ & \gcd(3,2) && 1 = 3 - 1\cdot 2 \\
& && \quad = (2\cdot 34 + (-5)\cdot 13) - 1\cdot(-3\cdot 34 + 8\cdot 13)) \\
& && \quad = 5\cdot 34 + (-13)\cdot 13
\end{aligned}
$$

Linear combinations

Definition 68 *An integer* r *is said to be a* linear combination *of a pair of integers* m *and* n *whenever*

> *there exist a pair of integers* s *and* t*, referred to as the* coefficients *of the linear combination, such that*

(DOT PRODUCT)

$$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \ ;$$

> *that is*

$$s \cdot m + t \cdot n = r \ .$$

Theorem 69 *For all positive integers* m *and* n*,*

1. $\gcd(\mathrm{m},\mathrm{n})$ *is a linear combination of* m *and* n*, and*
2. *a pair* $\mathrm{lc}_1(\mathrm{m},\mathrm{n})$*,* $\mathrm{lc}_2(\mathrm{m},\mathrm{n})$ *of integer coefficients for it, i.e. such that*

$$\left[\begin{array}{cc} \mathrm{lc}_1(\mathrm{m},\mathrm{n}) & \mathrm{lc}_2(\mathrm{m},\mathrm{n}) \end{array}\right] \cdot \left[\begin{array}{c} \mathrm{m} \\ \mathrm{n} \end{array}\right] = \gcd(\mathrm{m},\mathrm{n}) \quad ,$$

can be efficiently computed.

NB: There is an infinite number of coefficients expressing an integer as a linear combination of other two, as for all integers s, t, m, n, r:

$$s \cdot m + t \cdot n = r$$

If

for all integers k,

$$(s + kn) \cdot m + (t - km)\, n = r \,.$$

Proposition 70 *For all integers* m *and* n*,*

1. $\begin{bmatrix} 1 & 0 \\ ? & ? \end{bmatrix} \cdot \begin{bmatrix} \mathrm{m} \\ \mathrm{n} \end{bmatrix} = \mathrm{m} \quad \wedge \quad \begin{bmatrix} 0 & 1 \\ ? & ? \end{bmatrix} \cdot \begin{bmatrix} \mathrm{m} \\ \mathrm{n} \end{bmatrix} = \mathrm{n}$;

Proposition 70 *For all integers* m *and* n,

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \ \wedge \ \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

2. *for all integers* s_1, t_1, r_1 *and* s_2, t_2, r_2,

$$\begin{bmatrix} s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 \ \wedge \ \begin{bmatrix} s_2 & t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_2$$

implies

$$\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \ ;$$

Proposition 70 *For all integers* m *and* n,

1. $\begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \quad \wedge \quad \begin{bmatrix} 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

2. *for all integers* s_1, t_1, r_1 *and* s_2, t_2, r_2,

$$\begin{bmatrix} s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 \quad \wedge \quad \begin{bmatrix} s_2 & t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_2$$

implies

$$\begin{bmatrix} s_1+s_2 & t_1+t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \ ;$$

3. *for all integers* k *and* s, t, r,

$$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \ \textit{implies} \ \begin{bmatrix} rs & rt \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = k \cdot r \ .$$

Extended Euclid's Algorithm

We extend Euclid's Algorithm gcd(m,n) from computing on pairs of positive integers to computing on pairs of triples $((s,t),r)$ with s,t integers and r a positive integer satisfying the invariant that s,t are coefficients expressing r as an integer linear combination of m and n.

gcd

```
fun  gcd( m , n )
= let
    fun  gcditer( ((s1,t1) , r1) ,  c as ((s2,t2) , r2) )
    = let
        val (q,r) = divalg(r1,r2)   (* r = r1-q*r2 *)
      in
        if r = 0
        then  c
        else  gcditer(  c , ((s1-qs2 , t1-qt2) , r ))
      end
  in
    gcditer( ((1,0),m) , ((0,1),n) )
  end
```

NB: For positive integers m and n, egcd(m,n) outputs triples ((s,t),r) with $sm+tn=r=gcd(m,n)$.

```
fun egcd( m , n )
= let
    fun egcditer( ((s1,t1),r1) , lc as ((s2,t2),r2) )
    = let
        val (q,r) = divalg(r1,r2)   (* r = r1-q*r2 *)
      in
        if r = 0
        then lc
        else egcditer( lc , ((s1-q*s2,t1-q*t2),r) )
      end
  in
    egcditer( ((1,0),m) , ((0,1),n) )
  end
```

NB : $lc_1(m,n) \cdot m + lc_2(m,n) \cdot n = gcd(m,n)$

```
fun gcd( m , n ) = #2( egcd( m , n ) )

fun lc1( m , n ) = #1( #1( egcd( m , n ) ) )

fun lc2( m , n ) = #2( #1( egcd( m , n ) ) )
```

Multiplicative inverses in modular arithmetic

Corollary 74 *For all positive integers* m *and* n*,*

1. $\mathrm{n} \cdot \mathrm{lc}_2(\mathrm{m}, \mathrm{n}) \equiv \gcd(\mathrm{m}, \mathrm{n}) \pmod{\mathrm{m}}$*, and*
2. *whenever* $\gcd(\mathrm{m}, \mathrm{n}) = 1$*,*

   $\left[\mathrm{lc}_2(\mathrm{m}, \mathrm{n})\right]_{\mathrm{m}}$ *is the multiplicative inverse of* $[\mathrm{n}]_{\mathrm{m}}$ *in* $\mathbb{Z}_{\mathrm{m}}$.