Extended Euclid's Algorithm

Example 86

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

NB: gcd(34,13) is an int. lin. comb. of 34 and 13.

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

Integer linear combinations

Definition 64[a] 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

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

that is

$$s \cdot m + kmn - kmn + tn = s \cdot m + t \cdot n = r \;.$$

$$(s + kn) \cdot m + (t - km) n$$

[a] See page 194.

Theorem 87 *For all positive integers* m *and* n*,*

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

$$\begin{bmatrix} \mathrm{lc}_1(m, n) & \mathrm{lc}_2(m, n) \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = \gcd(m, n) \quad ,$$

can be efficiently computed.

Proposition 88 *For all integers* m *and* n,

1. $\begin{bmatrix} \overset{1}{\cancel{?_1}} & \overset{0}{\cancel{?_2}} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \;\; \wedge \;\; \begin{bmatrix} \overset{0}{\cancel{?_1}} & \overset{1}{\cancel{?_2}} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

$$?_1 \cdot m + ?_2 \cdot n = m$$

e.g. $?_1 = 1$, $?_2 = 0$

Remark: The coefficients expressing int. lin. comb. are not necessarily unique.

Proposition 88 *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

$$\begin{bmatrix} \overset{s_1+s_2}{\cancel{?_1}} & \overset{t_1+t_2}{\cancel{?_2}} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \;;$$

$$?_1 \cdot m + ?_2 \cdot n = r_1 + r_2 = s_1 \cdot m + t_1 n + s_2 \cdot m + t_2 \cdot n$$

$$= (s_1 + s_2)\, m + (t_1 + t_2) \cdot n$$

Proposition 88 *For all integers* m *and* n,

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

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

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

implies

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

3. *for all integers* k *and* s, t, r, $\quad k \cdot s \quad k \cdot t$

$$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \text{ implies } \begin{bmatrix} \cancel{?_1} & \cancel{?_2} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = k \cdot r \;.$$

$((1,0),m)$ $((0,1),n)$

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 coefficientes 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-q*s2 , t1-q*t2),r))
      end
  in
    gcditer( ((1,0),m) , ((0,1),n) )
  end
```

egcd

```
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
```

ML notation

$$\#1(a,b) = a$$
$$\#2(a,b) = b$$

```
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 ) ) )
```

$$\underline{gcd}(m,n) = \underline{lc_1}(m,n) \cdot m + \underline{lc_2}(m,n) \cdot n$$

For $\underline{gcd}(m,n)=1$, we have:

$$\underline{lc_1}(m,n) \cdot m + \underline{lc_2}(m,n) \cdot n = 1$$

FLT: $i \cdot i^{p-2} \equiv 1 \pmod{p}$ i not a mult. of p

Multiplicative inverses in modular arithmetic

Corollary 92 *For all positive integers* m *and* n,

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

2. *whenever* $\gcd(m,n) = 1$,

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

Natural Numbers and mathematical induction

We have mentioned in passing that the natural numbers are generated from zero by succesive increments. This is in fact the defining property of the set of natural numbers, and endows it with a very important and powerful reasoning principle, that of *Mathematical Induction*, for establishing universal properties of natural numbers.

Principle of Induction

Let $P(m)$ be a statement for m ranging over the set of natural numbers $\mathbb{N}$.

If

- the statement $P(0)$ holds, and
- the statement

  $$\forall n \in \mathbb{N}.\ \big(\ P(n) \implies P(n+1)\ \big)$$

  also holds

then

- the statement

  $$\forall m \in \mathbb{N}. P(m)$$

  holds.

Binomial Theorem

Theorem 29 *For all* $n \in \mathbb{N}$,

$$P(n) \stackrel{\text{def}}{=} \left[(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k \right].$$

PROOF: By induction,

Base $n=0$: That is, RTP:

$$(x+y)^0 \stackrel{?}{=} \sum_{k=0}^{0} \binom{0}{k} \cdot x^{-k} \, y^k$$

$$\shortparallel \qquad\qquad\qquad \shortparallel$$

$$1 \quad = \quad \binom{0}{0} x^0 y^0$$

Inductive step: Let $n \in \mathbb{N}$.

Assume

$$\text{(IH)} \quad (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Show

$$(x+y)^{n+1} \stackrel{?}{=} \sum_{k=0}^{n+1} \underbrace{\binom{n+1}{k}}_{= \left[\binom{n}{k} + \binom{n}{k-1}\right]} x^{n+1-k} y^k$$

$$= (x+y) \cdot (x+y)^n$$

$$\stackrel{\text{by (IH)}}{=} (x+y) \cdot \left(\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k\right)$$

$$= \sum_{k=0}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^{k+1}$$

$$\sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$$

$$= \sum_{k=0}^{n+1} \left[\binom{n}{k} + \binom{n}{k-1} \right] x^{n+1-k} y^k$$

$$= \sum_{n=0}^{n+1} \binom{n}{k} x^{n+1-k} y^k + \sum_{k=0}^{n+1} \binom{n}{k-1} x^{n+1-k} y^k$$

$= \ldots$ exercise ...

$\boxtimes$

Principle of Induction

from basis ℓ

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.

If

- $P(\ell)$ holds, and
- $\forall\, n \geq \ell$ in $\mathbb{N}$. $\big(P(n) \implies P(n+1) \big)$ also holds

then

- $\forall\, m \geq \ell$ in $\mathbb{N}$. $P(m)$ holds.