

### Extended Euclidean Algorithm (pseudocode version)

The following algorithm will compute the GCD of two polynomials  $f, g$  as well as linear combination  $sf + tg = GCD(f, g)$  (and more information). **Important convention:**  $LC(f) :=$  to the leading coefficient of  $f$ , and we define  $LC(0) = 1$ .

**Input:**  $f, g$  polynomials.

**Output:** Integer  $l$ , polynomials  $p_i, r_i, s_i, t_i$  for  $0 \leq i \leq l+1$ , and polynomial  $q_i$  for  $1 \leq i \leq l$ , such that  $s_i f + t_i g = r_i$ , and in particular,  $s_l f + t_l g = r_l = GCD(f, g)$ .

- Set  $p_0 := LC(f)$ ;  $p_1 := LC(g)$ ;  $r_0 := f/p_0$ ;  $r_1 := g/p_1$ ;
- Set  $s_0 := 1/p_0$ ;  $t_0 := 0$ ;  $s_1 := 0$ ;  $t_1 := 1/p_1$ ;
- $i:=1$ ; (counter);
- While  $r_i \neq 0$  do
  - $q_i := r_{i-1}$  quotient  $r_i$ ;
  - $p_{i+1} := LC(r_{i-1} - q_i r_i)$ ;
  - $r_{i+1} := (r_{i-1} - q_i r_i)/p_{i+1}$ ;
  - $s_{i+1} := (s_{i-1} - q_i s_i)/p_{i+1}$ ;
  - $t_{i+1} := (t_{i-1} - q_i t_i)/p_{i+1}$ ;
  - $i := i + 1$ ;
- od;
- $l:=i-1$ ;
- *RETURN*( $l, p_i, r_i, s_i, t_i, q_i$ );