- GCD - greatest common divisor - polynomial, of the highest possible degree, that is a factor of both the two original polynomials

Ex:

$$a = d^2 + 7d + 6$$

$$b = d^2 - 5d - 6$$

1) find roots of polynomials:

$$a: \quad d_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-7 \pm \sqrt{49 - 4 \cdot 1 \cdot 6}}{2 \cdot 1} = \frac{-7 \pm \sqrt{25}}{2} = \begin{cases} -1 \\ -6 \end{cases}$$

$$a = (d+1) \cdot (d+6)$$

$$b = (d+1) \cdot (d-6)$$

$$g = gcd(a, b) = d + 1$$

Is this approach effective? Yes, but only for quadratic equations (see the formula for calculating roots of cubic equation)

- GCD - how to calculate effectively?

=> Extended Euclidean algorithm

Theory: greatest common divisor $g = gcd(a, b)$ can be expressed by using the Bézout's lemma as in:

$$a \cdot p + b \cdot q = g$$

where

$g = gcd(a, b)$ .... greatest common divisor

a, b ..... known (input) polynomials. We are looking for the gcd of these polynomials

p, q .... pair of unknown coprime polynomials. Two polynomials are coprime if and only if they share no roots. Hence, $gcd(p, q) = 1$.

Similarly, the least common multiple $l = \mathrm{lcm}(a,b)$ can be expressed by using coprime polynomials pair r, s as in:

$$l = \mathrm{lcm}(a,b) = a \cdot r = -b \cdot s$$

Hence

$$a r + b \cdot s = 0$$

again $\gcd(r,s) = 1 \Rightarrow$ polynomials r, s are coprime.

Now we have two equations:

$$a \cdot p + b \cdot q = g$$

$$a \cdot r + b \cdot s = 0$$

In matrix form:

$$\begin{bmatrix} a & b \end{bmatrix} \cdot \begin{bmatrix} p & r \\ q & s \end{bmatrix} = \begin{bmatrix} g & 0 \end{bmatrix}$$

However, we also want to obtain polynomials p, q, r, s.
$\Rightarrow$ Multiplication by identity matrix:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} p & r \\ q & s \end{bmatrix} = \begin{bmatrix} p & r \\ q & s \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} p & r \\ q & s \end{bmatrix} = \begin{bmatrix} g & 0 \\ p & r \\ q & s \end{bmatrix}$$

! Extended Euclidean algorithm computes "output" matrix $\begin{bmatrix} g & 0 \\ p & r \\ q & s \end{bmatrix}$ out of "input" matrix $\begin{bmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$. How? By aplying a sequence of column operations on the input matrix.

Extended Euclidean algorithm's overview:

Function: Calculate $\begin{bmatrix} g & 0 \\ p & r \\ q & s \end{bmatrix}$ out of $\begin{bmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$, where

a, b are input polynomials; g is gcd of input polynomials; and p, q and r, s are coprime polynomials pairs.

$g = gcd(a, b)$

$l = lcm(a, b) = a \cdot r = -b \cdot s$

$gcd(p, q) = 1$

$gcd(r, s) = 1$

Allowed columns operations:

→ columns can be exchanged

$$[c_1 \quad c_2] \sim [c_2 \quad c_1]$$

Syntax of this operation:

$c_1(k+1) = c_2(k)$ ... column c_1 in algorithm's step $k+1$ is equal to column c_2 in algorithm's step k

$c_2(k+1) = c_1(k)$ ... column c_2 in algorithm's step $k+1$ is equal to column c_1 in algorithm's step k

Ex:

$$\begin{bmatrix} d+1 & d+2 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \overset{\substack{c_1(k+1) = c_2(k) \\ c_2(k+1) = c_1(k)}}{\sim} \begin{bmatrix} d+2 & d+1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$$

→ arbitrary column can be multiplied with nonzero constant

$$\begin{bmatrix} c_1 & c_2 \end{bmatrix} \sim \begin{bmatrix} \alpha \cdot c_1 & c_2 \end{bmatrix}$$

Syntax of this operation:

$c_1(k+1) = \alpha \cdot c_1(k)$ ... column c_1 in algorithm's step $k+1$ is equal to α-times column c_1 in algorithm's step k

Ex:

$$\begin{bmatrix} d+1 & d+2 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \overset{c_1(k+1)=5\cdot c_1(k)}{\sim} \begin{bmatrix} 5d+5 & d+2 \\ 5 & 0 \\ 0 & 1 \end{bmatrix}$$

→ any column can be multiplied with arbitrary polynomial and result can be added to second column

$$\begin{bmatrix} c_1 & c_2 \end{bmatrix} \sim \begin{bmatrix} c_1 & c_2 + x \cdot c_1 \end{bmatrix}$$

Syntax of this operation:

$c_2(k+1) = c_2(k) + x \cdot c_1(k)$ ... column c_2 in algorithm's step $k+1$ is equal to sum of c_2 in k and c_1 in k that is multiplied by polynomial x

Ex:

$$\begin{bmatrix} d+1 & d+2 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \overset{c_2(k+1) = c_2(k) + (d+1)c_1(k)}{\sim} \begin{bmatrix} d+1 & d^2+3d+3 \\ 1 & d+1 \\ 0 & 1 \end{bmatrix}$$

Ex: Find $\gcd(a, b)$, where

$$a = d^2 + 7d + 6$$

$$b = d^2 - 5d - 6$$

$$\begin{bmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} d^2+7d+6 & d^2-5d-6 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

We want to find

$$\begin{bmatrix} g & 0 \\ p & r \\ q & s \end{bmatrix}$$ in this position must be 0

$$\begin{bmatrix} d^2+7d+6 & d^2-5d-6 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \underset{C_2(1) = C_2(0) - C_1(0)}{\sim} \begin{bmatrix} d^2+7d+6 & -12d-12 \\ 1 & -1 \\ 0 & 1 \end{bmatrix} \underset{C_2(2) = \frac{-1}{12} C_2(1)}{\sim}$$

$$\begin{bmatrix} d^2+7d+6 & d+1 \\ 1 & \frac{1}{12} \\ 0 & -\frac{1}{12} \end{bmatrix} \underset{C_1(3) = C_1(2) - d \cdot C_2(2)}{\sim} \begin{bmatrix} 6d+6 & d+1 \\ 1-\frac{1}{12}d & \frac{1}{12} \\ \frac{1}{12}d & -\frac{1}{12} \end{bmatrix} \underset{C_1(4) = \frac{1}{6} \cdot C_1(3)}{\sim}$$

$$\begin{bmatrix} d+1 & d+1 \\ \frac{1}{6}-\frac{1}{72}d & \frac{1}{12} \\ \frac{1}{72}d & -\frac{1}{12} \end{bmatrix} \underset{C_2(5) = C_2(4) - C_1(4)}{\sim} \begin{bmatrix} d+1 & 0 \\ \frac{1}{6}-\frac{1}{72}d & \frac{1}{72}d-\frac{1}{12} \\ \frac{1}{72}d & -\frac{1}{72}d-\frac{1}{12} \end{bmatrix} = \begin{bmatrix} g & 0 \\ p & r \\ q & s \end{bmatrix}$$

$$\boxed{g = \gcd(a, b) = d + 1}$$

Ex: Are polynomials a,b coprime?

$$a = d+1$$

$$b = d^2+d-2$$

$$\begin{bmatrix} d+1 & d^2+d-2 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{matrix} c_2(1) = c_2(0) - d \cdot c_1(0) \\ \sim \end{matrix} \begin{bmatrix} d+1 & -2 \\ 1 & -d \\ 0 & 1 \end{bmatrix} \begin{matrix} c_2(2) = \frac{1}{-2} c_2(1) \\ \sim \end{matrix}$$

$$\begin{bmatrix} d+1 & 1 \\ 1 & \frac{d}{2} \\ 0 & -\frac{1}{2} \end{bmatrix} \begin{matrix} c_1(3) = c_1(2) - d \cdot c_2(2) \\ \sim \end{matrix} \begin{bmatrix} 1 & 1 \\ 1-\frac{d^2}{2} & \frac{d}{2} \\ \frac{d}{2} & -\frac{1}{2} \end{bmatrix} \begin{matrix} c_2(4) = c_2(3) - c_1(3) \\ \sim \end{matrix}$$

$$\begin{bmatrix} 1 & 0 \\ 1-\frac{d^2}{2} & \frac{d^2}{2}+\frac{d}{2}-1 \\ \frac{d}{2} & -\frac{d}{2}-\frac{1}{2} \end{bmatrix} = \begin{bmatrix} g & 0 \\ p & r \\ q & s \end{bmatrix}$$

$g = \gcd(a,b) = 1$ ... yes polynomials a,b are coprime

Ex: What is the least common multiple of a, b

$$a = d+1$$
$$b = d^2+d-2$$

(see previous example)...

$$r = \frac{d^2}{2} + \frac{d}{2} - 1$$

$$s = -\frac{d}{2} - \frac{1}{2}$$

$$l = \operatorname{lcm}(a,b) = a \cdot r = (d+1)\cdot\left(\frac{d^2}{2}+\frac{d}{2}-1\right) =$$
$$= \frac{d^3}{2} + \frac{d^2}{2} - d + \frac{d^2}{2} + \frac{d}{2} - 1 = \frac{d^3}{2} + d^2 - \frac{d}{2} - 1$$

$$l = \operatorname{lcm}(a,b) = -b \cdot s = (d^2+d-2)\cdot\left(\frac{d}{2}+\frac{1}{2}\right) =$$
$$= \frac{d^3}{2} + \frac{d^2}{2} - d + \frac{d^2}{2} + \frac{d}{2} - 1 = \frac{d^3}{2} + d^2 - \frac{d}{2} - 1$$