Fast matrix computation of subresultant polynomial remainder sequences *

Alkiviadis G. Akritas and Gennadi I. Malaschonok †
University of Thessaly (Greece), Tambov University (Russia)

Abstract

We present an improved (faster) variant of the matrix-triangularization subresultant prs method for the computation of a greatest common divisor of two polynomials A and B (of degrees d_A and d_B, respectively) along with their polynomial remainder sequence [1]. The computing time of our fast method is $O(n^{2+\beta} \log \|C\|^2)$, for standard arithmetic and $O(((n^{1+\beta} + n^3 \log \|C\|)(\log n + \log \|C\|)^2)$ for the Chinese remainder method, where $n = d_A + d_B$, $\|C\|$ is the maximal coefficient of the two polynomials and the best known $\beta < 2.356$. By comparison, the computing time of the old version is $O(n^5 \log \|C\|^2)$.

Our improvement is based on the work of Malaschonok [11] who proposed a new, recursive method for the solution of systems of linear equations in integral domains with complexity $O(n^\beta)$ over the integers (same as the complexity of matrix multiplication).

In this paper we present an overview of the two methods mentioned above and show how they are combined into a fast matrix method for computing polynomial remainder sequences. An example is also presented to clarify the concepts.

1 Introduction

Let Z be an integral domain, and let

$$A_i = \sum_{j=1}^{m} c_{ij} x^{m-j},$$

where $c_{ij} \in Z$, $i = 1, 2, \ldots, n$; then

$$mat(A_1, A_2, \ldots, A_n)$$

*This paper was published in the book *Computer Algebra in Scientific Computing - CASC 2000*, (Ed. by V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov), Springer, 2000, 1–11.

†Akritas is on leave from the University of Kansas, USA

denotes the matrix (c_{ij}) of order $n \times m$. Moreover, let $A, B \in Z[x], \deg A = d_A, \deg B = d_B$ and let

$$\begin{aligned} M_k &= mat(x^{d_B-k-1}A, x^{d_B-k-2}A, \ldots, A, x^{d_A-k-1}B, x^{d_A-k-2}B, \ldots, B), \\ & \quad 0 \leq k < \min(d_A, d_B) \end{aligned}$$

be the matrix of order $(d_A + d_B - 2k) \times (d_A + d_B - k)$, where M_0 is the well-known Sylvester's matrix. Then, kth subresultant polynomial of A and B is called the polynomial

$$S_k = \sum_{i=0}^{k} M_k^i x^i,$$

of degree $\leq k$, where M_k^i is a minor of the matrix M_k of order $d_A + d_B - 2k$, formed by the elements of columns $1, 2, \ldots, d_A + d_B - 2k - 1$ and column $d_A + d_B - k - i$. Habicht's known theorem [8] establishes a relation between the subresultant polynomials $S_0, S_1, \ldots, S_{\min(d_A, d_B)-1}$ and the polynomial remainder sequence(prs) of A and B, and also demonstrates the so-called *gap* structure.

According to the matrix-triangularization subresultant prs method (see for example Akritas' book [2] or papers [3], [4]) all the subresultant polynomials of A and B can be computed *within sign* by transforming the matrix (suggested by Sylvester [13])

$$mat(x^{\max(d_A,d_B)-1}A, x^{\max(d_A,d_B)-1}B, x^{\max(d_A,d_B)-2}A, x^{\max(d_A,d_B)-2}B, \ldots, A, B),$$

of order $2 \cdot \max(d_A, d_B)$, into its upper triangular form with the help of Dodgson's integer preserving transformations [7]; they are then located using an extension of a theorem by Van Vleck [3], [14]. (We depart from established practice and we give credit to Dodgson, and not to Bareiss [5], for the integer preserving transformations; see also the work of Waugh and Dwyer [15] where they use the same method as Bareiss, but 23 years earlier, and they name Dodgson as their source–differing from him only in the choice of the pivot element ([15], page 266). Charles Lutwidge Dodgson (1832–1898) is the same person widely known for his writing *Alice in Wonderland* under the pseudonym Lewis Carroll.)

In Section 2 we present an overview of the matrix-triangularization subresultant prs method allowing us to *exactly* compute and locate the members of the prs (*without* using Van Vleck's theorem [14]) by applying Dodgson's integer preserving transformations to a matrix of order $d_A + d_B$.

In Section 3 we present an overview of the recursive method for the solution of systems of linear equations in integral domains. Its complexity is the same as that of matrix multiplication.

In Section 4 we prove that the recursive method allowing us to compute and locate the members of the prs and gcd.

In Section 5 we present an example to clarify the concepts.

2 The "slow" matrix computation of subresultant polynomial remainder sequences

We assume that $\deg A = d_A \geq \deg B = d_B$ and we denote by M the following matrix

$$M = mat(x^{d_A-1}B, x^{d_A-2}B, \ldots, x^{d_B-1}B,^{d_B-1} A, x^{d_B-2}B, x^{d_B-2}A, \ldots, B, A)$$

of order $d_A + d_B$ with elements $a_{ij}(j, i = 1, 2, \ldots, d_A + d_B)$. (This matrix can be obtained from Sylvester's matrix M_0 after a rearrangement of its rows.)

Dodgson's integer preserving transformations

$$a_{ij}^{k+1} = \frac{(a_{ij}^k a_{kk}^k - a_{ik}^k a_{kj}^k)}{a_{k-1,k-1}^{k-1}} \qquad \text{(D)}$$

(see [5], [7], [9] or [15]) where we set $a_{00}^0 = 1$, $a_{ij}^1 = a_{ij}$ and it is assumed that $a_{kk}^k \neq 0, k = 1, 2, \ldots, d_A + d_B$, are applied to the matrix $M = (a_{ij})$ and transform it to the upper-triangular matrix $M_D = (b_{ij}), (i, j = 1, 2, \ldots, d_A + d_B)$, where

$$b_{ij} = \begin{cases} 0 & \text{for } i > j \\ a_{ij}^i & \text{for } i \leq j \end{cases}$$

and, in general,

$$a_{ij}^k = \begin{vmatrix} a_{11} & \ldots & a_{1,k-1} & a_{1j} \\ \vdots & \ddots & \vdots & \vdots \\ a_{k-1,1} & \ldots & a_{k-1,k-1} & a_{k-1,j} \\ a_{i1} & \ldots & a_{i,k-1} & a_{ij} \end{vmatrix}$$

with $1 \leq k \leq d_A + d_B$, and $k \leq i,\ j \leq d_A + d_B$.

The upper-triangular matrix $M_D = (b_{ij})$ will be called Dodgson matrix.

The following two theorems can be used to locate the members of the prs in the rows of M_D. The *correct* sign is computed.

Case 1: If none of the diagonal minors of the matrix M is equal to zero, then we have:

Theorem 1. Dodgson's integer preserving transformation will transform matrix M to the upper triangular matrix M_D, which contains all n subresultants (located in rows $d_A + d_B - 2k, k = 0, 1, 2, \ldots, d_B - 1$) $S_k = \sum_{i=0}^{k} M_k^i x^i$,

$$M_k^i = (-1)^{\sigma(k)} a_{d_A+d_B-2k, d_A+d_B-k-i}^{d_A+d_B-2k}$$

and $\sigma(k) = (d_A - d_B + 1) + \cdots + (d_A - k) = (1/2)(d_B - k)(2d_A - d_B - k + 1),\ k = 0, 1, \ldots, d_B - 1$.

Case 2: If *not* all diagonal minors of the matrix M are nonzero, then we have the following theorem (the term *bubble pivot*, used below, means that, after pivoting, row i_p is *immediately* below row j_p):

Theorem 2. Dodgson's integer preserving transformations with *bubble pivot* and choice of the pivot element by column, will transform matrix M to the upper triangular matrix M_D, and at the same time will compute all subresultants S_k; if, in the process, s row replacements take place, namely row j_1 replaces row i_1, j_2 replaces i_2, ..., j_s replaces i_s, (and after each replacement row i_p is immediately below row j_p, $p = 1, 2, \ldots, s$), then **(a)** $S_k = 0$, for all k such that $\frac{(d_A+d_B-i_p)}{2} > k > \frac{(d_A+d_B-j_p)}{2}$ and for all $p = 1, 2, \ldots, s$. **(b)** for all $p = 1, 2, \ldots, s$, if $k = \frac{(d_A+d_B-i_p)}{2}$ is an integer number not in (a), S_k is located in row i_p *before* it is replaced by row j_p. **(c)** for the remaining k, ($k = 0, 1, \ldots, d_B - 1$ and those not in (a) or (b)) S_k is located in row $j = d_A + d_B - 2k$.

Moreover, in (b) and (c) the subresultant $S_k = \sum_{i=0}^{k} M_k^i x^i$, is located in row j in such a way that

$$M_k^i = (-1)^{\sigma(k)+\sigma(j)} a^j_{j,j+k-i}$$

$\sigma(k) = (1/2)(d_B - k)(2d_A - d_B - k + 1)$, $\sigma(j) = \sum_{p=1}^{s} j_p - \sum_{p=1}^{s} i_p$, $j_p \le j$, $i_p \le j$.

Note that in cases (b) and (c) Theorem 2 reduces to Theorem 1 in the case of a complete prs, and due to the fact that rows above row j change places, the sign changes by a factor $(-1)^{\sigma(j)}$.

For the given polynomials over the integers in this discussion, the complexity of this method is

$$O(n^5 \log \|C\|^2))$$

where $n = d_A + d_B$ and $\|C\|$ is the maximal coefficient of the two polynomials.

3 The recursive method

Let $\sum_{j=1}^{m-1} a_{ij} x_j = a_{im}$, $i = 1, 2, \ldots, n$ be the system of linear equations with extended coefficients matrix

$$A = (a_{ij}),\ i = 1, \ldots, n,\ j = 1, \ldots, m.$$

whose coefficients are in integral domain $\mathbf{Z}$: $A \in \mathbf{Z}^{n \times m}$.

The solution of such a system may be written according to Cramer's rule

$$x_j = \frac{\delta^n_{jm} - \sum_{p=n+1}^{m-1} x_p \delta^n_{jp}}{\delta^n},\ j = 1, \ldots, n,$$

where x_p, $p = n+1, \ldots, m$, are free variables and $\delta^n \neq 0$. $\delta^n = |a_{ij}|$, $i = 1, \ldots, n$, $j = 1, \ldots, n$, - denote the corner minors of the matrix A of order n, δ^n_{ij} - denote the minors obtained by a substitution of the column j of the matrix A instead of the column i in the minors δ^n, $i = 1, \ldots, n$, $j = n+1, \ldots, m$. So we need to construct an algorithm for computing the minor δ^n and the matrix $G = (\ \delta^n_{ij}\ )$, $i = 1, \ldots, n$, $j = n+1, n+2, \ldots, m$.

This means that we must make the reduction of the matrix A to the diagonal form

$$A \rightarrow (\delta^n I_n, G).$$

I_n denotes the unit matrix of order n.

For the extended coefficients matrix $\mathbf{A}$ we use the following notation:

$$\mathbf{A}_{ij}^k = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,k-1} & a_{1j} \\ a_{21} & a_{22} & \cdots & a_{2,k-1} & a_{2j} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k-1,1} & a_{k-1,2} & \cdots & a_{k-1,k-1} & a_{k-1,j} \\ a_{i1} & a_{i2} & \cdots & a_{i,k-1} & a_{ij} \end{pmatrix}$$

is the matrix, formed by surrounding the sub-matrix of order $k-1$ in the upper left corner by row i and column j,

$$a_{ij}^k = \det \mathbf{A}_{ij}^k,$$

$a_{ij}^1 = a_{ij}$, $\delta^0 = 1$, $\delta^k = a_{kk}^k$, δ_{ij}^k is the determinant of the matrix, that is obtained from the matrix $\mathbf{A}_{kk}^k$ after the substitution of column i by column j.

We shall use the minors δ_{ij}^k and a_{ij}^k for the construction of the matrices

$$A_{k,c}^{r,l,(p)} = \begin{pmatrix} a_{r+1,k+1}^p & a_{r+1,k+2}^p & \cdots & a_{r+1,c}^p \\ a_{r+2,k+1}^p & a_{r+2,k+2}^p & \cdots & a_{r+2,c}^p \\ \vdots & \vdots & \ddots & \vdots \\ a_{l,k+1}^p & a_{l,k+2}^p & \cdots & a_{l,c}^p \end{pmatrix}$$

and

$$G_{k,c}^{r,l,(p)} = \begin{pmatrix} \delta_{r+1,k+1}^p & \delta_{r+1,k+2}^p & \cdots & \delta_{r+1,c}^p \\ \delta_{r+2,k+1}^p & \delta_{r+2,k+2}^p & \cdots & \delta_{r+2,c}^p \\ \vdots & \vdots & \ddots & \vdots \\ \delta_{l,k+1}^p & \delta_{l,k+2}^p & \cdots & \delta_{l,c}^p \end{pmatrix}$$

$G_{k,c}^{r,l,(p)}, A_{k,c}^{r,l,(p)} \in \mathbf{Z}^{(l-r)\times(c-k)}$, $0 \le k < n$, $k < c \le n$, $0 \le r < m$, $r < l \le m$, $1 \le p \le n$.

We describe one recursive step, that makes the following reduction of the matrix $\tilde{A}$ to the diagonal form

$$\tilde{A} \to (\delta^l I_{l-k}, G_{l,c}^{k,l,(l)}),\ 0 \le k < c \le m,\ k < l \le n,\ l < c.$$

Note that if $k = 0$, $l = n$ and $c = m$, then we obtain the solution of the system.

We choose the arbitrary integer number s: $k < s < l$ and write the matrix $\tilde{A} = A_{k,c}^{s,l,(k+1)}$ as follows:

$$\tilde{A} = \begin{pmatrix} A_{k,c}^{k,s(k+1)} \\ A_{k,c}^{s,l,(k+1)} \end{pmatrix}$$

where $A_{k,c}^{k,s,(k+1)}$ is the upper part of the matrix $\tilde{A}$ consisting of $s-k$ rows and $A_{k,c}^{s,l,(k+1)}$ is the lower part of the matrix $\tilde{A}$.

The first step

We make the following reduction of the matrix $A_{k,c}^{k,s(k+1)} \in \mathbf{Z}^{(s-k)\times(c-k)}$ to the diagonal form

$$A_{k,c}^{k,s(k+1)} \to (\delta^s I_{s-k}, G_{s,c}^{k,s,(s)}).$$

The second step

We write the matrix $A^{s,l,(k+1)}_{k,c}$ in the following way:

$$A^{s,l,(k+1)}_{k,c} = (A^{s,l,(k+1)}_{k,s}, A^{s,l,(s+1)}_{s,c})$$

where $A^{s,l,(k+1)}_{k,s}$ consists of the first $s-k$ columns and $A^{s,l,(k+1)}_{s,c}$ consists of the last $c-s$ columns of the matrix $A^{s,l,(k+1)}_{k,c}$.

The matrix $A^{s,l,(s+1)}_{s,c}$ is obtained from the matrix identity:

$$\delta^k \cdot A^{s,l,(s+1)}_{s,c} = \delta^s \cdot A^{s,l,(k+1)}_{s,c} - A^{s,l,(k+1)}_{k,s} \cdot G^{k,s,(s)}_{s,c}.$$

The minors δ^k must not equal zero.

The third step

As the next recursive step we make the following reduction of the matrix $A^{s,l,(s+1)}_{s,c} \in \mathbf{Z}^{(l-s)\times(c-s)}$ to the diagonal form

$$A^{s,l,(s+1)}_{s,c} \to (\delta^l I_{l-s}, G^{s,l,(l)}_{l,c}).$$

The fourth step

We write the matrix $G^{k,s,(s)}_{s,c}$ in the following way:

$$G^{k,s,(s)}_{s,c} = (G^{k,s,(s)}_{s,l}, G^{k,s,(s)}_{l,c})$$

where $G^{k,s,(s)}_{s,l}$ consists of the first $l-s$ columns and $G^{k,s,(s)}_{l,c}$ consists of the last $c-l$ columns of the matrix $G^{k,s,(s)}_{s,c}$.

The matrix $G^{k,s,(l)}_{l,c}$ is obtained from the matrix identity:

$$\delta^s \cdot G^{k,s,(l)}_{l,c} = \delta^l \cdot G^{k,s,(s)}_{l,c} - G^{k,s,(s)}_{s,l} \cdot G^{s,l,(l)}_{l,c}.$$

The minors δ^s must not equal zero.

So we get

$$G^{k,l,(l)}_{l,c} = \begin{pmatrix} G^{k,s,(l)}_{l,c} \\ G^{s,l,(l)}_{l,c} \end{pmatrix}$$

and δ^l.

3.1 Representation of the one recursive step

We can represent one recursive step as the following reduction of the matrix $A^{kl(k+1)}_{kc}$:

$$A^{kl(k+1)}_{kc} = \begin{pmatrix} A^{k,s(k+1)}_{k,c} \\ A^{s,l,(k+1)}_{k,c} \end{pmatrix} \to_1 \begin{pmatrix} \delta^s I_{s-k} & G^{ks(s)}_{sc} \\ A^{s,l,(k+1)}_{k,s} & A^{s,l,(k+1)}_{s,c} \end{pmatrix} \to_2 \begin{pmatrix} \delta^s I_{s-k} & G^{ks(s)}_{sc} \\ 0 & A^{sl(s+1)}_{sc} \end{pmatrix} \to_3$$

$$\to_3 \begin{pmatrix} \delta^s I_{s-k} & G^{ks(s)}_{sl} & G^{ks(s)}_{lc} \\ 0 & \delta^l I_{l-s} & G^{sl(l)}_{lc} \end{pmatrix} \to_4 \begin{pmatrix} \delta^s I_{s-k} & 0 & G^{ks(l)}_{lc} \\ 0 & \delta^l I_{l-s} & G^{sl(l)}_{lc} \end{pmatrix} \to \begin{pmatrix} \delta^l I_{s-k} & G^{kl(l)}_{lc} \end{pmatrix}$$

4 Dichotomous recursion

If the process of partition is dichotomous, and the number of rows in the upper and lower submatrixes is the same and equal to a power of 2 in every step, then we will call such process - the dichotomous recursion process.

Let us denote

$$A_k^{2^p} = A_{kc}^{k,k+2^p(k+1)}, \quad G_k^{2^p} = G_{kc}^{k-2^p,k(k)}$$

matrices with 2^p rows and $c-k$ columns. For any natural number s we denote by $b[s]$ the maximal power of 2, that devide the nubmer s, i.e. for $s = \sum_{i=0}^{j} c_i 2^i, c_i \in \{0,1\}$ $b[s] = 2^w$, where $w = min\{i|c_i \neq 0\}$.

Then one dichotomous recursive step is as follows:

$$A_{t2^p}^{2^p} \to_1 \begin{pmatrix} \delta^{(2t+1)2^{p-1}} I_{2^{p-1}} & G_{(2t+1)2^{p-1}}^{2^{p-1}} \\ * & * \end{pmatrix} \to_2 \begin{pmatrix} \delta^{(2t+1)2^{p-1}} I_{2^{p-1}} & G_{(2t+1)2^{p-1}}^{2^{p-1}} \\ 0 & A_{(2t+1)2^{p-1}}^{2^{p-1}} \end{pmatrix}$$

$$\to_3 \begin{pmatrix} * & * & * \\ 0 & \delta^{(t+1)2^p} I_{2^{p-1}} & G_{(t+1)2^p}^{2^{p-1}} \end{pmatrix} \to_4 \left(\delta^{(t+1)2^p} I_{2^p} \quad G_{(t+1)2^p}^{2^p} \right)$$

$$p = 1, 2, \ldots, N, \quad t = 0, 1, \ldots, 2^{N-p} - 1, \quad n = 2^N.$$

We obtain the following sequense of matrices:

A_0^2; G_2^2, A_2^2; G_4^2, G_4^4, A_4^4; G_6^2, A_6^2, G_8^2, G_8^4, G_8^8, A_8^8; G_{10}^2, A_{10}^2, G_{12}^2, G_{12}^4, A_{12}^4, G_{14}^2, A_{14}^2, G_{16}^2, G_{16}^4, G_{16}^8, $G_{16}^{16}, \ldots$ $A_{4s}^{b[4s]}$, G_{4s+2}^2, A_{4s+2}^2, G_{4s+4}^2, $G_{4s+4}^4, \ldots, G_{4s+4}^{b[4s+4]}, \ldots$
which we call the *dichotomous sequence of matrices.*

Theorem 3. The dichotomous sequence of matrices contains all the rows of the Dodgson matrix M_D.

Proof: The dichotomous sequence of matrices includes the matrices $A_t^{b[t]}$, $t = 2, 4, \ldots, n-2$, $\quad G_t^2$, $t = 2, 4, \ldots, n$.

The matrix $A_t^{b[t]}$, $t = 2, 4, \ldots, n-2$, has the next first row

$$(a_{t+1,t+1}^{t+1}, a_{t+1,t+2}^{t+1}, \ldots, a_{t+1,m}^{t+1}),$$

the matrix G_t^2, $t = 2, 4, \ldots, n-2$, has the next last row

$$(\delta_{t,t}^t, \delta_{t,t+1}^t, \ldots, \delta_{t,m}^t) = (a_{t,t}^{t+1}, a_{t,t+1}^{t+1}, \ldots, a_{t,m}^{t+1})$$

.

There are rows of the Dodgson matrix M_D with the numbers $t+1$ ($t = 2, 4, \ldots, n-2$) and t ($t = 2, 4, \ldots, n$) respectively. So the dichotomous sequence of matrices contains all the rows of the Dodgson matrix M_D . □

Therefore, we can use the dichotomous sequence of matrices for computing the Dodgson matrix with the prs's and gcd.

Comparing with Dodgson's method, care must be taken not to make bubble-pivot in each row with zero diagonal element but just in the even rows, because just the diagonal elements in the even rows will be the pivots. Details can be seen in the example that follows – taken from our previous paper [1].

5 Complexity issue

Let $\|C\|$ denote the maximal coefficient of the two polynomials, n^β denote the complexity of matrix multiplication of order n, $n = d_A + d_B$, where d_A and d_B are the degrees of the two polynomials. The best known $\beta < 2.356$. Since the fast method of matrix transformation required n^β operations with integer numbers so it is easy to obtain the complexity of our method.

Our method is required

$$O(n^{2+\beta} \log^2 \|C\|)$$

bit operations for standard arithmetic and

$$O(((n^{1+\beta} + n^3 \log \|C\|)(\log n + \log \|C\|)^2)$$

for the Chinese remainder method. The cost of reducing modulo a prime is included.

6 Example of Fast Matrix Transformation

We present an example to clarify the concepts discussed above. It is the same example taken from our previous paper [1].

For the polynomials

$$\begin{aligned} A &= 2x^4 + 5x^3 + 5x^2 - 2x + 1 \\ B &= 3x^3 + 3x^2 + 3x - 4 \end{aligned}$$

we obtain the following matrices:

$$\begin{pmatrix} 3 & 3 & 3 & -4 & 0 & 0 & 0 \\ 2 & 5 & 5 & -2 & 1 & 0 & 0 \\ 0 & 3 & 3 & 3 & -4 & 0 & 0 \\ 0 & 2 & 5 & 5 & -2 & 1 & 0 \\ 0 & 0 & 3 & 3 & 3 & -4 & 0 \\ 0 & 0 & 2 & 5 & 5 & -2 & 1 \\ 0 & 0 & 0 & 3 & 3 & 3 & -4 \end{pmatrix} \to_1 \begin{pmatrix} 9 & 0 & 0 & -14 & -3 & 0 & 0 \\ 0 & 9 & 9 & 2 & 3 & 0 & 0 \\ 0 & 3 & 3 & 3 & -4 & 0 & 0 \\ 0 & 2 & 5 & 5 & -2 & 1 & 0 \\ 0 & 0 & 3 & 3 & 3 & -4 & 0 \\ 0 & 0 & 2 & 5 & 5 & -2 & 1 \\ 0 & 0 & 0 & 3 & 3 & 3 & -4 \end{pmatrix} \to_2$$

$$\begin{pmatrix} 9 & 0 & 0 & -14 & -3 & 0 & 0 \\ 0 & 9 & 9 & 2 & 3 & 0 & 0 \\ 0 & 0 & 0 & 21 & 45 & 0 & 0 \\ 0 & 0 & 27 & 41 & -24 & 9 & 0 \\ 0 & 0 & 3 & 3 & 3 & -4 & 0 \\ 0 & 0 & 2 & 5 & 5 & -2 & 1 \\ 0 & 0 & 0 & 3 & 3 & 3 & -4 \end{pmatrix} \to_3 \begin{pmatrix} 9 & 0 & 0 & -14 & -3 & 0 & 0 \\ 0 & 9 & 9 & 2 & 3 & 0 & 0 \\ 0 & 0 & -63 & 0 & -149 & -21 & 0 \\ 0 & 0 & 0 & -63 & 135 & 0 & 0 \\ 0 & 0 & 3 & 3 & 3 & -4 & 0 \\ 0 & 0 & 2 & 5 & 5 & -2 & 1 \\ 0 & 0 & 0 & 3 & 3 & 3 & -4 \end{pmatrix}$$

$$\to_4 \begin{pmatrix} -63 & 0 & 0 & 0 & 231 & 0 & 0 \\ 0 & -63 & 0 & 0 & 98 & 21 & 0 \\ 0 & 0 & -63 & 0 & -149 & -21 & 0 \\ 0 & 0 & 0 & -63 & 135 & 0 & 0 \\ 0 & 0 & 3 & 3 & 3 & -4 & 0 \\ 0 & 0 & 2 & 5 & 5 & -2 & 1 \\ 0 & 0 & 0 & 3 & 3 & 3 & -4 \end{pmatrix} \to_5$$

$$\begin{pmatrix} -63 & 0 & 0 & 0 & 231 & 0 & 0 \\ 0 & -63 & 0 & 0 & 98 & 21 & 0 \\ 0 & 0 & -63 & 0 & -149 & -21 & 0 \\ 0 & 0 & 0 & -63 & 135 & 0 & 0 \\ 0 & 0 & 0 & 0 & -147 & 315 & 0 \\ 0 & 0 & 0 & 0 & -692 & 168 & -63 \\ 0 & 0 & 0 & 0 & -594 & -189 & 252 \end{pmatrix} \to_6$$

$$\begin{pmatrix} -63 & 0 & 0 & 0 & 231 & 0 & 0 \\ 0 & -63 & 0 & 0 & 98 & 21 & 0 \\ 0 & 0 & -63 & 0 & -149 & -21 & 0 \\ 0 & 0 & 0 & -63 & 135 & 0 & 0 \\ 0 & 0 & 0 & 0 & -3068 & 0 & -315 \\ 0 & 0 & 0 & 0 & 0 & -3068 & -147 \\ 0 & 0 & 0 & 0 & -594 & -189 & 252 \end{pmatrix} \to_7$$

$$\begin{pmatrix} -63 & 0 & 0 & 0 & 231 & 0 & 0 \\ 0 & -63 & 0 & 0 & 98 & 21 & 0 \\ 0 & 0 & -63 & 0 & -149 & -21 & 0 \\ 0 & 0 & 0 & -63 & 135 & 0 & 0 \\ 0 & 0 & 0 & 0 & -3068 & 0 & -315 \\ 0 & 0 & 0 & 0 & 0 & -3068 & -147 \\ 0 & 0 & 0 & 0 & 0 & 0 & 15683 \end{pmatrix}$$

The obtained polynomial remainder sequence is incomplete and we only have the remainder $-63x + 135$ of degree 1 after the thired step and remainder 15683 of degree 0 after the seventh step.

Matrix operations in the each step:

1. $\delta_2 = \begin{vmatrix} 3 & 3 \\ 2 & 5 \end{vmatrix} = 9; \begin{vmatrix} 3 & 3 \\ 2 & 5 \end{vmatrix} = 9; \begin{vmatrix} 3 & -4 \\ 2 & -2 \end{vmatrix} = 2; \begin{vmatrix} 3 & 0 \\ 2 & 1 \end{vmatrix} = 3; \begin{vmatrix} 3 & 0 \\ 2 & 0 \end{vmatrix} = 0;$
$\begin{vmatrix} 3 & 0 \\ 2 & 0 \end{vmatrix} = 0; \begin{vmatrix} 3 & 3 \\ 5 & 5 \end{vmatrix} = 0; \begin{vmatrix} -4 & 3 \\ -2 & 5 \end{vmatrix} = -14; \begin{vmatrix} 0 & 3 \\ 1 & 5 \end{vmatrix} = -3; \begin{vmatrix} 0 & 3 \\ 0 & 5 \end{vmatrix} = 0; \begin{vmatrix} 0 & 3 \\ 0 & 5 \end{vmatrix} = 0.$

2. $9\begin{pmatrix} 3 & 3 & -4 & 0 & 0 \\ 5 & 5 & -2 & 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 3 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & -14 & -3 & 0 & 0 \\ 9 & 2 & 3 & 0 & 0 \end{pmatrix} =$
$\begin{pmatrix} 0 & 21 & 45 & 0 & 0 \\ 27 & 41 & -24 & 9 & 0 \end{pmatrix}.$

3. $\delta_4 = \begin{vmatrix} 0 & 21 \\ 27 & 41 \end{vmatrix}\frac{1}{9} = -63; \begin{vmatrix} 0 & -45 \\ 27 & -24 \end{vmatrix}\frac{1}{9} = 135; \begin{vmatrix} 0 & 0 \\ 27 & 9 \end{vmatrix}\frac{1}{9} = 0; \begin{vmatrix} 0 & 0 \\ 27 & 0 \end{vmatrix}\frac{1}{9} = 0;$
$\begin{vmatrix} -45 & 21 \\ -24 & 41 \end{vmatrix}\frac{1}{9} = -149; \begin{vmatrix} 0 & 21 \\ 9 & 41 \end{vmatrix}\frac{1}{9} = -21; \begin{vmatrix} 0 & 21 \\ 0 & 41 \end{vmatrix}\frac{1}{9} = 0.$

4. $\left((-63)\begin{pmatrix}-3 & 0 & 0\\ 3 & 0 & 0\end{pmatrix} - \begin{pmatrix}0 & -14\\ 9 & 2\end{pmatrix}\begin{pmatrix}-149 & -21 & 0\\ 135 & 0 & 0\end{pmatrix}\right)\frac{1}{9} = \begin{pmatrix}231 & 0 & 0\\ 98 & 21 & 0\end{pmatrix}.$

5. $(-63)\begin{pmatrix}3 & -4 & 0\\ 5 & -2 & 1\\ 3 & 3 & -4\end{pmatrix} - \begin{pmatrix}0 & 0 & 3 & 3\\ 0 & 0 & 2 & 5\\ 0 & 0 & 0 & 3\end{pmatrix}\begin{pmatrix}231 & 0 & 0\\ 98 & 21 & 0\\ -149 & -21 & 0\\ 135 & 0 & 0\end{pmatrix} =$
$\begin{pmatrix}-147 & 315 & 0\\ -692 & 168 & -63\\ -594 & -189 & 252\end{pmatrix}.$

6. $\delta_6 = \frac{\begin{vmatrix}-147 & 315\\ -692 & 168\end{vmatrix}}{(-63)} = -3068; \quad \frac{\begin{vmatrix}-147 & 0\\ -692 & -63\end{vmatrix}}{(-63)} = -147; \quad \frac{\begin{vmatrix}0 & 315\\ -63 & 168\end{vmatrix}}{(-63)} = -315;$

7. $\delta_7 = (252(-3068) - (-315)(-594) - (147)(-189))/(-63) = 15683.$

References

[1] Akritas, A.G., Akritas, E.K. and Gennadi I. Malaschonok. *Matrix computation of subresultant polynomial remainder sequences in integral domains*. Reliable Computing **1** (1995), pp. 375–381.

[2] Akritas, A. G. *Elements of Computer Algebra with Applications*. J. Wiley Interscience, New York, 1989.

[3] Akritas, A. G. A new method for computing polynomial greatest common divisors and polynomial remainder sequences. Numerische Mathematik **52**, 119–127, 1988.

[4] Akritas, A. G. Exact algorithms for the matrix-triangularization subresultant prs method. Proceedings of the Conference on Computers and Mathematics, Boston, Massachusetts, 145–155, June 1989.

[5] Bareiss, E. H. Sylvester's identity and multistep integer-preserving Gaussian elimination. Mathematics of Computation **22**, 565–578, 1968.

[6] Coppersmith, D. and S. Winograd. in Proc. 19th Annu ACM Symp. on Theory of Comput., 1987, 1–6.

[7] Dodgson, C. L. Condensation of determinants. Proceedings of the Royal Society of London **15**. 150–155, 1866.

[8] Habicht, W. Eine Verallgemeinerung des Sturmschen Wurzelzaelverfahrens. Commentarii Mathematici Helvetici **21**, 99–116, 1948.

[9] Malaschonok, G. I. Solution of a system of linear equations in an integral domain. USSR Journal of Computational Mathematics and Mathematical Physics **23**, 1497–1500, 1983 (in Russian).

[10] G.I. Malaschonok. Algorithms for the solution of systems of linear equations in commutative rings. In *Effective Methods in Algebraic Geometry*, Edited by T. Mora and C. Traverso, Progress in Mathematics 94, Birkhauser, Boston-Basel-Berlin, 1991, 289–298.

[11] G. I. Malaschonok. Recursive Method for the Solution of systems of Linear Equations,*Computational Mathematics* (A. Sydow Ed, Proceedings of the 15th IMACS World Congress, Vol. I, Berlin, August 1997), Wissenschaft & Technik Verlag, Berlin 1997, 475–480.

[12] Strassen, V. Gaussian Elimination is not optimal. *Numerische Mathematik* **13**, 354–356, 1969.

[13] Sylvester, J. J. On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest common measure. Philoshophical Transactions **143**, 407–548, 1853.

[14] Van Vleck, E. B. On the determination of a series of Sturm's functions by the calculation of a single determinant. Annals of Mathematics **1**, Second Series, 1–13, 1899–1900.

[15] Waugh, F. V. and P. S. Dwyer Compact computation of the inverse of a matrix. Annals of Mathematical Statistics **16**, 259–271, 1945.