Serdica J. Computing **10** (2016), No 1, 31–48

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

A BASIC RESULT ON THE THEORY OF SUBRESULTANTS*

Alkiviadis G. Akritas, Gennadi I. Malaschonok, Panagiotis S. Vigklas

Abstract. Given the polynomials $f, g \in \mathbb{Z}[\mathbb{x}]$ the main result of our paper, Theorem 1, establishes a *direct* one-to-one correspondence between the modified Euclidean and Euclidean polynomial remainder sequences (prs's) of f, g computed in $\mathbb{Q}[\mathbb{x}]$, on one hand, and the subresultant prs of f, g computed by determinant evaluations in $\mathbb{Z}[\mathbb{x}]$, on the other.

An important consequence of our theorem is that the signs of Euclidean and modified Euclidean prs's — computed either in $\mathbb{Q}[\mathbb{x}]$ or in $\mathbb{Z}[\mathbb{x}]$ — are *uniquely* determined by the corresponding signs of the subresultant prs's. In this respect, *all* prs's are *uniquely* "signed."

Our result fills a gap in the theory of subresultant prs's. In order to place Theorem 1 into its correct historical perspective we present a brief historical review of the subject and hint at certain aspects that need — according to our opinion — to be revised.

ACM Computing Classification System (1998): F.2.1, G.1.5, I.1.2.

Key words: Euclidean algorithm, Euclidean polynomial remainder sequence (prs), modified Euclidean prs, subresultant prs, modified subresultant prs, Sylvester matrices, Bezout matrix, Sturm's prs.

*The second author was partially supported by RFBR grant No 16-07-00420a.

1. Introduction. In this section we *briefly* examine the historical development of the theory of subresultants and set the historical framework for our main result, Theorem 1. A detailed historical exposition of the subject can be found elsewhere [13].

We assume that the reader is familiar with the Euclidean algorithm applied on the polynomials f, g as well as with Sturm's algorithm, when $g = f'$ [20]; in case $g \neq f'$, the latter is called *modified* Euclidean algorithm. Next, we informally present subresultants since they are formally defined in almost all texts and articles on the subject [6], [12], [13], [14].

Consider the polynomials $f, g \in \mathbb{Z}[x]$ of degrees $deg(f) = n$ and $deg(g) = m$ with $n \geq m$. The *subresultant prs* of f, g is a sequence of polynomials in $\mathbb{Z}[x]$ analogous to the Euclidean prs, the sequence obtained by applying on f, g Euclid's algorithm for polynomial greatest common divisors (gcd) in $\mathbb{Q}[x]$.

The subresultant prs differs from the Euclidean prs in that the coefficients of each polynomial in the former sequence are the determinants — also referred to as *subresultants* — of appropriately selected sub-matrices of `sylvester1(f, g, x)`[1], Sylvester's matrix of 1840 of dimensions $(n + m) \times (n + m)$ [21].

Recall that the determinant of `sylvester1(f, g, x)` itself is called the *resultant* of f, g and serves as a criterion of whether the two polynomials have common roots or not [16], [20].

Likewise, the *modified subresultant prs* of f, g is a sequence of polynomials in $\mathbb{Z}[x]$ analogous to the *modified* Euclidean prs, the sequence obtained by applying in $\mathbb{Q}[x]$ Sturm's algorithm on f, g, where g may be different from f'.

The modified subresultant prs differs from the modified Euclidean prs in that the coefficients of each polynomial in the former sequence are the determinants — also referred to as the *modified subresultants* — of appropriately selected sub-matrices of `sylvester2(f, g, x)`, Sylvester's matrix of 1853 of dimensions $(2 \cdot n) \times (2 \cdot n)$ [22].

The determinant of `sylvester2(f, g, x)` is called *modified resultant* of f, g and it too can serve as a criterion of whether the two polynomials have common roots or not.

The use of matrices `sylvester1(f, g, x)` and `sylvester2(f, g, x)` is amply demonstrated elsewhere [4].

The discussion so far is partially summarized in Figure 1 below. The arrows and their labels are explained in the sequel.

Note on the matrices used in Figure 1. We have repeatedly stressed

[1]To distinguish it from `sylvester2(f, g, x)`, Sylvester's matrix of 1853 of dimensions $(2 \cdot n) \times (2 \cdot n)$ [22].

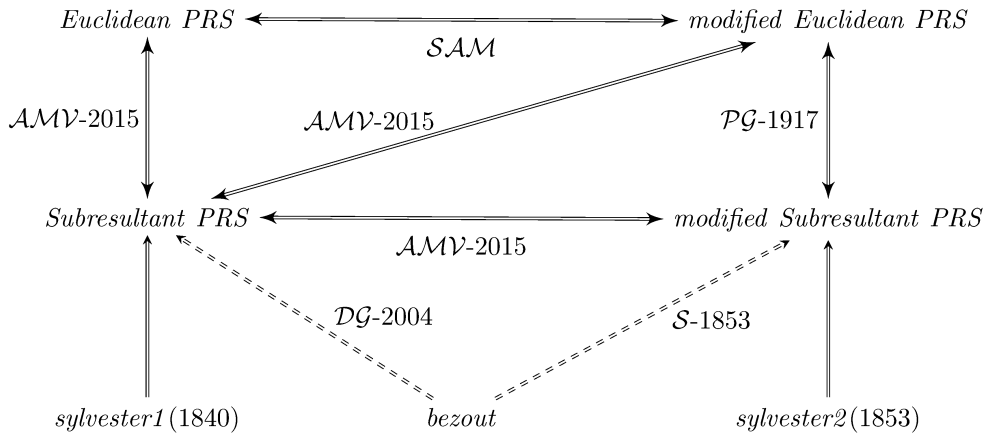

Fig. 1. The double-ended arrows indicate one-to-one correspondences that exist between the coefficients of the polynomials in the respective nodes. The labels indicate those who first established the correspondences and when. The dashed arrow labeled $\mathcal{DG}$-2004 is due to Diaz–Toca and Gonzalez–Vega [12], whereas the one labeled $\mathcal{S}$-1853 is due to Sylvester [22], [24].

in our work that `sylvester2(f, g, x)`, Sylvester's matrix of 1853, has not been given the attention it deserves. In this case, again, this matrix has been overshadowed in the literature by the so called Sylvester-Habicht matrix [6], of smaller dimensions. But if dimensions were the key factor for picking a matrix, why not pick the Bezout matrix of even smaller dimensions? The latter, appropriately rotated, is equivalent to `sylvester2(f, g, x)` [12].

For our discussion in the sequel we will need the following definitions.

Definition 1. *The* `sign sequence` *of a polynomial remainder sequence is the sequence of signs of the leading coefficients of its polynomials.*

Definition 2. *A polynomial remainder sequence of two polynomials f, g is called* `complete` *if the degree difference between any two consecutive polynomials is 1; otherwise, it is called* `incomplete`.[2]

For complete prs's it is well known that the sign sequence of the subresultant prs and that of the Euclidean prs are identical [1]. For such prs's it is also well known that the sign sequence of the modified subresultant prs and that of

[2]It is understood that f, g are included in the prs.

the modified Euclidean prs are identical. In either case, one can easily compute one prs from the other.

However, it is also well known that for incomplete prs's the sign sequence of the subresultant prs and that of the Euclidean prs are in general different. And likewise for the sign sequences of the modified subresultant prs and that of the modified Euclidean prs. Therefore, in either case, there was a big problem computing one prs from the other. Neither Sylvester himself nor Van Vleck were able to solve the problem [3], [24].

The solution to the above problem came from Anna Johnson Pell[3] and R. L. Gordon in 1917 [19]. In the statement of their theorem — which, by the way, uses the `sylvester2(f, g, x)` matrix — we have the *first* algorithm for the computation of modified subresultant prs's.

The Pell-Gordon algorithm had been dormant for about a century, but is now included in the `sympy` module `subresultants_qq_zz.py`[4] as function `modified_subresultants_pg(f, g, x)`.

Clearly, the Pell-Gordon theorem establishes a one-to-one correspondence between modified Euclidean prs's computed in $\mathbb{Q}[x]$ and modified subresultant prs's computed in $\mathbb{Z}[x]$. See the arrow labelled $\mathcal{PG}$-1917 in Figure 1.

This correspondence is easily extended to modified Euclidean prs's computed in $\mathbb{Z}[x]$ [4]. This is achieved by utilizing the function `rem_z(f, g, x)`, defined by

$$|\operatorname{LC}(g)|^{\delta} \cdot f = q \cdot g + h, \tag{1}$$

where h is the remainder, $\operatorname{LC}(g)$ is the leading coefficient of the divisor g, and

$$\delta = \operatorname{degree}(f, x) - \operatorname{degree}(g, x) + 1. \tag{2}$$

This one-to-one correspondence between modified Euclidean prs's and modified subresultant prs's (all in $\mathbb{Z}[x]$) was reinvented first by Habicht in 1948, [15], and, several decades later, by others [6], [18].

It is worth noting that Habicht *completely* avoided polynomial divisions in $\mathbb{Z}[x]$. Instead, his results are expressed via — what we now call — mod-

[3]For her fascinating biography see `https://en.wikipedia.org/wiki/Anna_Johnson_Pell_Wheeler`.

[4]Based on the Pell-Gordon theorem and on Theorem 1 we were able to develop algorithms for the computation of (modified) Euclidean and (modified) subresultant prs's, both in $\mathbb{Q}[\mathbb{x}]$ and $\mathbb{Z}[\mathbb{x}]$, utilizing respectively the functions `rem(f, g, x)` and `rem_z(f, g, x)`. The latter is defined in (1).

Our module is included in `sympy 1.0`; for earlier versions it can be found in `https://github.com/sympy/sympy/blob/master/sympy/polys/subresultants_qq_zz.py`. Obviously, the module can be `load`-ed or `attach`-ed in a `sage` session.

ified subresultants. In other words, without explicitly saying it, Habicht used `sylvester2(f, g, x)`.

Later researchers, [6], [18], followed a different approach. The matrix `sylvester2(f, g, x)` was bypassed in favor of the Sylvester-Habicht matrix and, for polynomial divisions in $\mathbb{Z}[x]$, instead of our function `rem_z(f, g, x)`, the so called "signed pseudo-remainder" function was employed ([6], p. 21); according to the latter, the dividend is pre-multiplied times $\mathrm{LC}(g)^{\delta_1}$, where $\delta_1 = \delta + 1$ if $\delta \bmod 2 = 1$.[5]

In other words, to *exactly* compute the signs of Euclidean and modified Euclidean prs's one has to completely *avoid* the pseudo-remainder function `prem(f, g, x)`, which was introduced by Collins, Brown and Traub [7], [8], [10], [11] and is defined by

$$\mathrm{LC}(g)^{\delta} \cdot f = q \cdot g + h. \tag{3}$$

Caveat. With the function `prem(f, g, x)` *only* the signs of subresultant prs's can be *exactly* computed ([9], pp. 277–283); the exact signs of Euclidean and modified Euclidean prs's *cannot* be computed with the pseudo-remainder function (3). See the literature [2], [7], [8], [10], [11], [13], [14], [17].

The arrow labelled $\mathcal{SAM}$ in Figure 1 indicates a one-to-one correspondence that exists between Euclidean prs's and modified Euclidean prs's. This is based on the observation made by Sylvester in 1853, [23], that the signs of the two sequences differ according to a certain pattern, a fact which is proved in Lemma 1, in Section 2.

The vertical and diagonal arrows labelled $\mathcal{AMV}$-2015 in Figure 1 are proved in Theorem 1.

Finally, the horizontal arrow labelled $\mathcal{AMV}$-2015 in Figure 1 indicates a one-to-one correspondence between subresultant prs's and modified subresultant prs's. As explained elsewhere [5], this correspondence was proved using a theorem by Diaz–Toca and Gonzalez–Vega [12].

1.1. Outline of the paper. In Section 2 we provide the necessary mathematical background for the proof of our major result which is then presented in Section 3.

In Section 4, we present an example which demonstrates the use of Theorem 1 in computing the coefficients of a modified Euclidean and a Euclidean prs with the help of the corresponding coefficients of the subresultant prs.

[5] Obviously, now the size of the coefficients increases even more than it does with `rem_z(f, g, x)`.

Finally in Section 5 we present our conclusions.

Our work is based on, and complements, the work by Pell and Gordon, [19], who showed how to compute the coefficients of incomplete modified Euclidean prs's using modified subresultants [4].

2. Preliminaries. To prove our main result we need the following lemmata. The first of these lemmata establishes the relation between Euclidean and modified Euclidean prs's.

Lemma 1. *Let*

$$r^s_{j-1} = q^s_j r^s_j + (-1)^s r^s_{j+1}, \quad \|r^s_j\| > \|r^s_{j+1}\|, \quad s = 0, 1, \ j = 0, 1, 2, \ldots.$$

be sequences of divisions with remainder in a polynomial ring $\mathbb{K}[x]$*, where* $\mathbb{K}$ *is a field. If for some number* $i \geq 0$ *the following equalities are true*

$$r^0_{i-1} = r^1_{i-1}, \qquad r^0_i = r^1_i, \tag{4}$$

then, for all $j > i$*, the following equalities are also true*

$$q^0_j = (-1)^{j-i} q^1_j, \qquad r^0_j = (-1)^{\pi_{i,j}} r^1_j, \quad \textit{where} \quad \pi_{i,j} = \lfloor (j - i + 1)/2 \rfloor. \tag{5}$$

P r o o f. By definition, the two sequences are formed as follows:

$$\begin{array}{lllllll}
r^0_{i-1} &=& q^0_i r^0_i + r^0_{i+1}, & & r^1_{i-1} &=& q^1_i r^1_i - r^1_{i+1}, \\
r^0_i &=& q^0_{i+1} r^0_{i+1} + r^0_{i+2}, & & r^1_i &=& q^1_{i+1} r^1_{i+1} - r^1_{i+2}, \\
r^0_{i+1} &=& q^0_{i+2} r^0_{i+2} + r^0_{i+3}, & & r^1_{i+1} &=& q^1_{i+2} r^1_{i+2} - r^1_{i+3}, \\
r^0_{i+2} &=& q^0_{i+3} r^0_{i+3} + r^0_{i+4}, & & r^1_{i+2} &=& q^1_{i+3} r^1_{i+3} - r^1_{i+4}.
\end{array}$$

From the above, taking into consideration condition (4), we obtain the following equalities:

$$\begin{array}{lllllll}
q^0_i &=& q^1_i, & & r^0_{i+1} &=& -r^1_{i+1}, \\
q^0_{i+1} &=& -q^1_{i+1}, & & r^0_{i+2} &=& -r^1_{i+2}, \\
q^0_{i+2} &=& q^1_{i+2}, & & r^0_{i+3} &=& r^1_{i+3}, \\
q^0_{i+3} &=& -q^1_{i+3}, & & r^0_{i+4} &=& r^1_{i+4}.
\end{array}$$

We see that the statement of the lemma is true for the first four remainders. Since it is true that $r^0_{i+3} = r^1_{i+3}$ and $r^0_{i+4} = r^1_{i+4}$, the statement of the lemma holds for the next four remainders as well, etc., until the end of the division algorithm with remainder. □

Consequences of Lemma 1. Let $\mathbb{K}[x]$ be a polynomial ring over the field $\mathbb{K}$, and $a, b \in \mathbb{K}[x] \backslash 0$. Then the remainder sequence r^0_j, obtained by applying Euclid's algorithm on a, b, and the remainder sequence r^1_j, obtained by applying Sturm's algorithm on a, b, satisfy the equation

$$r^0_j = (-1)^{\pi_j} r^1_j, \quad \text{where} \quad \pi_j = \lfloor (j + 1)/2 \rfloor, \quad j = 1, 2, \ldots. \tag{6}$$

Lemma 2. *Consider the list* $S_k = \{p_1, p_2, \ldots, p_k\}$ *of integer numbers. Denote by* s *the number of odd integers in* S_k *and by* s' *the number of odd integers in* $S_k \setminus p_1 = \{p_2, p_3, \ldots, p_k\}$. *Then, the following equalities hold:*

$$\text{(a)}\ \ \lfloor (s+1)/2 \rfloor \mod 2 = (\sum_{j=1}^{k} p_j^2 + \sum_{1 \le i < j \le k} p_i p_j) \mod 2,$$

$$\text{(b)}\ \ \lfloor (s+1)/2 \rfloor - \lfloor (s'+1)/2 \rfloor \mod 2 = p_1 \sum_{j=1}^{k} p_j \mod 2.$$

P r o o f. To prove part (a) of the Lemma consider the following obvious equalities:

$$2 \sum_{1 \le i < j \le k} p_i p_j + \sum_{j=1}^{k} p_j^2 = \left(\sum_{j=1}^{k} p_j \right)^2,$$

$$\left(\sum_{j=1}^{k} p_j \right)^2 \mod 2 = s^2 \mod 2;\ \ \sum_{j=1}^{k} p_j^2 \mod 2 = s \mod 2,$$

$$\sum_{1 \le i < j \le k} p_i p_j \mod 2 = (s^2 - s)/2 \mod 2 = \lfloor s/2 \rfloor \mod 2.$$

Part (b) follows immediately from part (a). □

3. Our main result.

Theorem 1. *Let*

$$\begin{aligned} f &= a_0 x^n + a_1 x^{n-1} + \cdots + a_n, \\ g &= b_0 x^n + b_1 x^{n-1} + \cdots + b_n \end{aligned} \tag{7}$$

be two polynomials of degree n *and* $n - p_0$, *respectively, with* $b_0 = b_1 = \cdots = b_{p_0 - 1} = 0$, $b_{p_0} \neq 0$, $p_0 \geq 0$. *Moreover, for* $i = 1, 2, \ldots$, *let*

$$\begin{aligned} R^{(i)} &= r_0^{(i)} x^{m_i} + r_1^{(i)} x^{m_i - 1} + \cdots + r_{m_i}^{(i)}, \\ R^{E(i)} &= r_0^{E(i)} x^{m_i} + r_1^{E(i)} x^{m_i - 1} + \cdots + r_{m_i}^{E(i)}, \end{aligned} \tag{8}$$

be the i*-th modified Euclidean and Euclidean remainders, respectively, of* f, g, *with* $R^{(i)}$ *and* $R^{E(i)}$ *both of degree* $m_i - p_i + 1$, *where* $(m_i + 1)$ *is the degree of the preceding remainder and*

$$r_0^{(i)} = r_0^{E(i)} = \cdots = r_{p_i - 2}^{(i)} = r_{p_i - 2}^{E(i)} = 0,\ \ \varrho_i = r_{p_i - 1}^{(i)} \neq 0,\ \ \sigma_i = r_{p_i - 1}^{E(i)} \neq 0.$$

Then for $k = 0, 1, \ldots, m_i$ *the coefficients* $r_k^{(i)}$ *and* $r_k^{E(i)}$ *in (8) are given by*

$$r_k^{(i)} = \frac{(-1)^{\varphi_i}}{\varrho_{i-1}^{p_{i-1}+1}\varrho_{i-2}^{p_{i-2}+p_{i-1}}\cdots\varrho_0^{p_0+p_1}} \times \frac{\mathrm{Det}_{i,k}(f,g)}{a_0^{p_0}}, \tag{9}$$

$$r_k^{E(i)} = \frac{(-1)^{\psi_i}}{\sigma_{i-1}^{p_{i-1}+1}\sigma_{i-2}^{p_{i-2}+p_{i-1}}\cdots\sigma_0^{p_0+p_1}} \times \frac{\mathrm{Det}_{i,k}(f,g)}{a_0^{p_0}}, \tag{10}$$

where $\varrho_0 = \sigma_0 = b_{p_0}$,

$$\varphi_i = \lfloor (s_{i-1}+1)/2 \rfloor, \tag{11}$$

$$s_{i-1} = \textit{the number of odd integers in the list } \{p_0, p_1, \ldots, p_{i-1}\}, \tag{12}$$

$$\psi_i = i + \varphi_i + p_1 + p_3 + p_5 + .. + p_{2\lfloor i/2 \rfloor - 1}, \ \textit{with } p_{-1} = 0, \tag{13}$$

$$\mathrm{Det}_{i,k}(f,g) = \begin{vmatrix}
a_0 & a_1 & \cdots & a_{p_0} & \cdots & a_{v_{i-1}} & \cdots & a_{2v_{i-1}} & a_{2v_{i-1}+k+1} \\
0 & a_0 & \cdots & a_{p_0-1} & \cdots & a_{v_{i-1}-1} & \cdots & a_{2v_{i-1}-1} & a_{2v_{i-1}+k} \\
\vdots & & \ddots & & \cdots & & \ddots & & \vdots \\
0 & 0 & \cdots & a_0 & \cdots & a_{v_{i-1}-p_0} & \cdots & a_{2v_{i-1}-p_0} & a_{2v_{i-1}+k+1-p_0} \\
\vdots & & \ddots & & \ddots & & \ddots & & \vdots \\
0 & 0 & \cdots & 0 & \cdots & a_0 & \cdots & a_{v_{i-1}} & a_{v_{i-1}+k+1} \\
b_0 & b_1 & \cdots & b_{p_0} & \cdots & b_{v_{i-1}} & \cdots & b_{2v_{i-1}} & b_{2v_{i-1}+k+1} \\
0 & b_0 & \cdots & b_{p_0-1} & \cdots & b_{v_{i-1}-1} & \cdots & b_{2v_{i-1}-1} & b_{2v_{i-1}+k} \\
\vdots & & \ddots & & \cdots & & \ddots & & \vdots \\
0 & 0 & \cdots & b_0 & \cdots & a_{v_{i-1}-p_0} & \cdots & a_{2v_{i-1}-p_0} & a_{2v_{i-1}+k+1-p_0} \\
\vdots & & \ddots & & \ddots & & \ddots & & \vdots \\
0 & 0 & \cdots & 0 & \cdots & b_0 & \cdots & b_{v_{i-1}} & b_{v_{i-1}+k+1}
\end{vmatrix}, \tag{14}$$

and

$$v_{i-1} = p_0 + p_1 + \cdots + p_{i-1}. \tag{15}$$

P r o o f. By structural induction on the polynomials in the prs.
We first consider the behavior of the modified Euclidean remainders.
Basis step: Setting $i = 1$ in expression (9) we obtain

$$r_k^{(1)} = \frac{(-1)^{\varphi_1}}{b_{p_0}^{p_0+1}} \times \frac{\mathrm{Det}_{1,k}(f,g)}{a_0^{p_0}}, \quad \text{where } \varphi_1 = p_0 \bmod 2, \quad \text{and}$$

$$\text{(16)}\qquad \mathrm{Det}_{1,k}\,(f,g)=\begin{vmatrix} a_0 & a_1 & \cdots & a_{p_0} & a_{p_0+1} & \cdots & a_{2p_0} & a_{2p_0+k+1} \\ 0 & a_0 & \cdots & a_{p_0-1} & a_{p_0} & \cdots & a_{2p_0-1} & a_{2p_0+k} \\ \vdots & & \ddots & & & \ddots & & \vdots \\ 0 & 0 & \cdots & a_0 & a_1 & \cdots & a_{p_0} & a_{p_0+k+1} \\ b_0 & b_1 & \cdots & b_{p_0} & b_{p_0+1} & \cdots & b_{2p_0} & b_{2p_0+k+1} \\ 0 & b_0 & \cdots & b_{p_0-1} & b_{p_0} & \cdots & b_{2p_0-1} & b_{2p_0+k} \\ \vdots & & \ddots & & & \ddots & & \vdots \\ 0 & 0 & \cdots & b_0 & b_1 & \cdots & b_{p_0} & b_{p_0+k+1} \end{vmatrix},$$

where the dimensions of the determinant are $(2p_0+2)\times(2p_0+2)$ and there are p_0 zero elements: $b_0=\ldots=b_{p_0-1}=0$.

Note that if $p_0=0$, we obtain

$$\text{(17)}\qquad r_k^{(1)}=\frac{1}{b_0}\times\mathrm{Det}_{1,k}\,(f,g)\,,\quad\text{where}\quad \mathrm{Det}_{1,k}\,(f,g)=\begin{vmatrix} a_0 & a_{k+1} \\ b_0 & b_{k+1} \end{vmatrix}.$$

The above expression is obvious, since if we divide f by g and take the negative of the remainder (Sturm's algorithm) we obtain

$$\text{(18)}\qquad R^{(1)}=r_0^{(1)}x^{n-1}+r_1^{(1)}x^{n-2}+\cdots+r_{n-1}^{(1)},$$

Denote, now, by A_0 the upper left block of $\mathrm{Det}_{1,k}(f,g)$, of dimensions $p_0\times p_0$. This is an upper triangular block with

$$\text{(19)}\qquad \mathrm{Det}(A)=a_0^{p_0}.$$

Moreover, since $b_0=\ldots=b_{p_0-1}=0$ the lower left block is zero. Therefore, we can write determinant (16) in block form as:

$$\text{(20)}\qquad \mathrm{Det}_{1,k}(f,g)=\begin{vmatrix} A_0 & B_0 \\ 0 & D_0 \end{vmatrix}.$$

To obtain the first remainder we have to perform p_0+1 steps. Denote by $a_i^{(j)}$ the coefficients of the partial remainders, where $a_i=a_i^{(0)}$ and $a_k^{(p_0+1)}=-r_{k-p_0-1}^{(1)}$, for $k\geq p_0+1$. We take remainders with inverse sign as in Sturm's algorithm.

From (19) and (20) we see that to prove the theorem for $i=1$, we need to show that $\mathrm{Det}(D_0)=(-1)^{\varphi_1}r_k^{(1)}b_{p_0}^{p_0+1}$, where

$$\text{(21)}\qquad D_0=\begin{pmatrix} a_0 & a_1 & \cdots & a_{p_0} & a_{p_0+k+1} \\ b_{p_0} & b_{p_0+1} & \cdots & b_{2p_0} & b_{2p_0+k+1} \\ 0 & b_{p_0} & \cdots & b_{2p_0-1} & b_{2p_0+k} \\ & & \ddots & & \vdots \\ 0 & 0 & \cdots & b_{p_0} & b_{p_0+k+1} \end{pmatrix}.$$

To prove the desired result, we left-multiply matrix D_0 times the matrices Y_i, $i = 0, 2, \ldots, p_0$, where each matrix Y_i is obtained from the identity matrix of size $p_0 + 2$ by adding the nonzero element $\dfrac{-a_i^{(i)}}{b_{p_0}}$ in column $i+1$ of the first row. In other words we have:

$$Y_0 = \begin{bmatrix} 1 & \dfrac{-a_0^{(0)}}{b_{p_0}} & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}, Y_1 = \begin{bmatrix} 1 & 0 & \dfrac{-a_1^{(1)}}{b_{p_0}} & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}, \ldots,$$

$$Y_{p_0} = \begin{bmatrix} 1 & 0 & \cdots & \dfrac{-a_{p_0}^{(p_0)}}{b_{p_0}} \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

The matrices $Y_0 \cdot D_0$, $Y_1 \cdot Y_0 \cdot D_0, \ldots$, $Y_{p_0} \cdots Y_0 \cdot D_0$ have in their *first* row the elements $[0, a_1^{(1)}, a_2^{(1)} \ldots]$, $[0, 0, a_2^{(2)}, a_3^{(2)}, \ldots]$, $\ldots$, $[0, 0, \ldots, 0, a_{p_0+k+1}^{(p_0+1)}]$, respectively. All others rows remain the same. Since $\mathrm{Det}(Y_i) = 1$, for all i, we have $\mathrm{Det}(D_0) = \mathrm{Det}(Y_{p_0} \cdots Y_0 D_0) = b_{p_0}^{b_{p_0}+1}(-1)^{p_0+1}(-r_k^{(1)})$.

Therefore we have proved the theorem for the case $i = 1$.

In the sequel, since the first coefficients of $R^{(i)}$ in (8) may be zero, we introduce the following special notation whereby we ignore the zero leading coefficients of the polynomial:

$$\bar{R}^{(i)} = \bar{r}_0^{(i)} x^{m_i - p_i + 1} + \bar{r}_1^{(i)} x^{m_i - p_i} + \cdots + \bar{r}_{m_i - p_i + 1}^{(i)}, \ (\bar{r}_0^{(i)} = r_{p_i - 1}^{(i)}).$$

In particular, we are interested in the function

$$\bar{R}^{(0)} = \bar{g} = \bar{b}_0 x^{n-p_0} + \bar{b}_1 x^{n-p_0-1} + \cdots + \bar{b}_{n-p_0}, \ (\bar{b}_0 = b_{p_0}). \tag{22}$$

Recursive step: Assume Theorem 1 is true for any pair of polynomials in the prs and, hence, for $\bar{g}, R^{(1)}$ as well. Then, applying the statement of the theorem to the pair of polynomials $\bar{g}, R^{(1)}$ we have:

$$r'^{(i)}_k = (-1)^{\varphi'_i} (\varrho_{i-1}^{p_{i-1}+1} \varrho_{i-2}^{p_{i-2}+p_{i-1}} \cdots \varrho_1^{p_1+p_2} \varrho_0^{p_1})^{-1} \, \mathrm{Det}_{i,k}\left(\bar{g}, R^{(1)}\right), \tag{23}$$

$$\varphi'_i = \lfloor (s'_{i-1} + 1)/2 \rfloor,$$

$$s'_{i-1} = \text{the number of odd integers in the list } \{p_1, \ldots, p_{i-1}\},$$

$$(24)\quad \mathrm{Det}_{i,k}(\bar{g}, R^{(1)}) = \begin{vmatrix} \bar{b}_0 & \bar{b}_1 & \bar{b}_2 & \cdots & \bar{b}_{V_{i-1}} & \bar{b}_{V_{i-1}+1} & \cdots & \bar{b}_{2V_{i-1}} & \bar{b}_{2V_{i-1}+k+1} \\ 0 & \bar{b}_0 & \bar{b}_1 & \cdots & \bar{b}_{V_{i-1}-1} & \bar{b}_{V_{i-1}} & \cdots & \bar{b}_{2V_{i-1}-1} & \bar{b}_{2V_{i-1}+k} \\ \vdots & & & \ddots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & \bar{b}_0 & \bar{b}_1 & \cdots & \bar{b}_{V_{i-1}} & \bar{b}_{V_{i-1}+k+1} \\ 0 & r_0^{(1)} & r_1^{(1)} & \cdots & r_{V_{i-1}-1}^{(1)} & r_{V_{i-1}}^{(1)} & \cdots & r_{2V_{i-1}}^{(1)} & r_{2V_{i-1}+k+1}^{(1)} \\ 0 & 0 & r_0^{(1)} & \cdots & r_{V_{i-1}-2}^{(1)} & r_{V_{i-1}-1}^{(1)} & \cdots & r_{2V_{i-1}-1}^{(1)} & r_{2V_{i-1}+k}^{(1)} \\ \vdots & & & \ddots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & r_0^{(1)} & r_1^{(1)} & \cdots & r_{V_{i-1}-1}^{(1)} & r_{V_{i-1}+k+2}^{(1)} \\ 0 & 0 & 0 & \cdots & 0 & r_0^{(1)} & \cdots & r_{V_{i-1}}^{(1)} & r_{V_{i-1}+k+1}^{(1)} \end{vmatrix}$$

of dimensions $(2V_{i-1}+2) \times (2V_{i-1}+2)$ and

$$V_{i-1} = p_1 + \cdots + p_{i-1}.$$

We will express determinant (14) as a function of determinant (24), and show that equation (23) reduces to equation (9).

In (14), denote by A the upper left block of $\mathrm{Det}_{i,k}(f,g)$, of dimensions $p_0 \times p_0$. This is an upper triangular block with $\mathrm{Det}(A) = a_0^{p_0}$. Since $b_0 = \ldots = b_{p_0-1} = 0$ the lower left block is zero. Therefore, we can write determinant (14) in block form as:

$$(25)\qquad \mathrm{Det}_{i,k}(f,g) = \begin{vmatrix} A & B \\ 0 & D \end{vmatrix},$$

where

$$(26)\qquad D = \begin{bmatrix} a_0 & \cdots & a_{v_{i-1}-p_0} & \cdots & a_{v_{i-1}} & \cdots & a_{2v_{i-1}-p_0} & a_{2v_{i-1}+k+1-p_0} \\ & \ddots & & \ddots & & \vdots & & \\ 0 & \cdots & a_0 & \cdots & a_{p_0} & \cdots & a_{v_{i-1}} & a_{v_{i-1}+k+1} \\ b_{p_0} & \cdots & b_{v_{i-1}} & \cdots & b_{v_{i-1}+p_0} & \cdots & b_{2v_{i-1}} & b_{2v_{i-1}+k+1} \\ & \ddots & & & & \ddots & & \vdots \\ 0 & \cdots & b_{p_0} & \cdots & b_{2p_0} & \cdots & b_{v_{i-1}+p_0} & b_{v_{i-1}+k+1+p_0} \\ & \ddots & & \ddots & & & & \vdots \\ 0 & \cdots & 0 & \cdots & b_{p_0} & \cdots & b_{v_{i-1}} & b_{v_{i-1}+k+1} \end{bmatrix}.$$

Left-multiplying matrix D times matrices Y_i of appropriate dimensions, we obtain

matrix D',

$$D' = \begin{bmatrix}
0 & \cdots & r_0^{(1)} & \cdots & r_{v_{i-1}-1-p_0}^{(1)} & r_{v_{i-1}-p_0}^{(1)} & \cdots & r_{2v_{i-1}-2p_0-1}^{(1)} & r_{2v_{i-1}+k-2p_0}^{(1)} \\
 & \cdots & & \ddots & & & \vdots & & \\
0 & \cdots & 0 & \cdots & r_0^{(1)} & r_1^{(1)} & \cdots & r_{v_{i-1}-p_0}^{(1)} & r_{v_{i-1}+k+1-p_0}^{(1)} \\
0 & \cdots & 0 & \cdots & 0 & r_0^{(1)} & \cdots & r_{v_{i-1}-1-p_0}^{(1)} & r_{v_{i-1}+k-p_0}^{(1)} \\
b_{p_0} & \cdots & b_{2p_0+1} & \cdots & b_{v_{i-1}+p_0} & b_{v_{i-1}+p_0+1} & \cdots & b_{2v_{i-1}} & b_{2v_{i-1}+k+1} \\
0 & \cdots & b_{2p_0} & \cdots & b_{v_{i-1}+p_0-1} & b_{v_{i-1}+p_0} & \cdots & b_{2v_{i-1}-1} & b_{2v_{i-1}+k} \\
 & \cdots & & \ddots & & \vdots & & & \\
0 & \cdots & 0 & \cdots & b_{2p_0} & b_{2p_0+1} & \cdots & b_{v_{i-1}+p_0} & b_{v_{i-1}+k+1+p_0} \\
 & \cdots & & \ddots & & & & & \vdots \\
0 & \cdots & 0 & \cdots & b_{p_0} & b_{p_0+1} & \cdots & b_{v_{i-1}} & b_{v_{i-1}+k+1}
\end{bmatrix},$$

with $\mathrm{Det}(D') = (-1)^{v_{i-1}+1-p_0} \cdot \mathrm{Det}(D)$. The sign $(-1)^{v_{i-1}+1-p_0}$ appears as a result of the sign inversion in the polynomial coefficients $R^{(1)}$ in the firsts $v_{i-1} + 1 - p_0$ rows.

In matrix D' interchange the upper group of rows with the lower group of rows; this will result in $\mathrm{Det}(D') = (-1)^{(v_{i-1}+1)(v_{i-1}+1-p_0)} \cdot \mathrm{Det}(D')$.

Decompose now D' into four blocks, so that the upper left block is of dimensions $p_0 \times p_0$ with determinant $b_{p_0}^{p_0}$. This way, the lower left corner is the zero matrix, whereas in the lower right corner is matrix $\mathrm{Det}_{i,k}\left(\bar{g}, R^{(1)}\right)$.

It is easy to see that $(-1)^{v_{i-1}+1-p_0}(-1)^{(v_{i-1}+1)(v_{i-1}+1-p_0)} = (-1)^{v_{i-1}p_0}$. Hence, since $b_{p_0} = \varrho_0$, we obtain the determinant identity

$$\mathrm{Det}_{i,k}(f, g) = (-1)^{v_{i-1}p_0}(a_0\varrho_0)^{p_0}\,\mathrm{Det}_{i,k}(\bar{g}, R^{(1)}). \tag{27}$$

Moreover, due to Lemma 2 we obtain the equality $(-1)^{\varphi-\varphi'} = (-1)^{v_{i-1}p_0}$.

Therefore, $r'^{(i)}_k = r^{(i)}_k$, and we have just proved equation (9) of the theorem.

To prove equation (10) we use Lemma 1, which states that for all $j > 0$, we have

$$\sigma_j = (-1)^{\lfloor (j+1)/2 \rfloor}\varrho_j = (-1)^{j(j+1)/2}\varrho_j,$$

and, hence,

$$\varrho_{k-1}^{p_{k-1}+p_k}\varrho_k^{p_k+p_{k+1}} = \sigma_{k-1}^{p_{k-1}+p_k}\sigma_k^{p_k+p_{k+1}}(-1)^{(p_{k-1}(k-1)k+2p_kk^2+p_{k+1}k(k+1))/2}.$$

Substituting in the first fraction in (9) results in

$$(28)\quad \frac{(-1)^{\varphi_i}}{(\varrho_{i-1}^{p_{i-1}+1}\varrho_{i-2}^{p_{i-2}+p_{i-1}}\cdots\varrho_1^{p_1+p_2}\varrho_0^{p_1})} = \frac{(-1)^{\varphi_i}(-1)^{(i-1)i/2+\sum_{k=0}^{\lfloor i/2\rfloor-1}p_{2k+1}(2k+1)^2}}{(\sigma_{i-1}^{p_{i-1}+1}\sigma_{i-2}^{p_{i-2}+p_{i-1}}\cdots\sigma_1^{p_1+p_2}\sigma_0^{p_1})},$$

from which we obtain (10). □

4. Example. Consider the storied polynomials $f = x^8+x^6-3x^4-3x^3+8x^2+2x-5$ and $g = 3x^6+5x^4-4x^2-9x+21$, whose incomplete polynomial remainder sequence (prs) has degrees $8, 6, 4, 2, 1, 0$.

The subresultant prs of f, g in $\mathbb{Z}[x]$ is

$$(29)\quad x^8+x^6-3x^4-3x^3+8x^2+2x-5, 3x^6+5x^4-4x^2-9x+21,$$
$$15x^4-3x^2+9, 65x^2+125x-245, 9326x-12300, 260708,$$

where the coefficients of the polynomials in the second row of (29) are all determinants (*subresultants*) of appropriately selected sub-matrices of `sylvester1`, of dimensions 16×16.

Given (29) we will compute the coefficients of the modified Euclidean and the Euclidean prs's with the help of (9) and (10).

First we compute the coefficients of the modified Euclidean prs. These coefficients are the rational numbers shown in (30) below and were computed using polynomial divisions in $\mathbb{Q}[x]$.

$$(30)\quad x^8+x^6-3x^4-3x^3+8x^2+2x-5, 3x^6+5x^4-4x^2-9x+21,$$
$$5x^4/9-x^2/9+1/3, 117x^2/25+9x-441/25,$$
$$233150x/19773-102500/6591, -1288744821/543589225.$$

To start the process of computing the coefficients of (30) using the subresultants obtained from (29), note that for the polynomials f, g of our example we have $a_0 = 1$, $\varrho_0 = 3$ and $p_0 = 2$, in which case $s_0 = 0$, and $\varphi_1 = \lfloor (s_0+1)/2\rfloor = 0$.

To compute the first non-zero coefficient of the first remainder, that is $\frac{5}{9}$, we set $i = 1$, and from (29) we see that the value of the corresponding determinant, $\mathrm{Det}_{1,1}(f,g)$, is 15 — since $\mathrm{Det}_{1,0}(f,g) = 0$ and, hence, $r_0^{(1)} = 0$. Then, from (9) we have that

$$\varrho_1 = r_1^{(1)} = \frac{(-1)^{\varphi_1}}{\varrho_0^{p_0+1}}\times \mathrm{Det}_{1,1}(f,g) = \frac{(-1)^0}{3^{2+1}}\times 15 = \frac{15}{27} = \frac{5}{9}.$$

The other two coefficients of the first remainder are

$$r_3^{(1)} = \frac{(-1)^{\varphi_1}}{\varrho_0^{p_0+1}}\times \mathrm{Det}_{1,3}(f,g) = \frac{(-1)^0}{3^{2+1}}\times(-3) = \frac{-3}{27} = -\frac{1}{9},$$

and

$$r_5^{(1)} = \frac{(-1)^{\varphi_1}}{\varrho_0^{p_0+1}} \times \mathrm{Det}_{1,5}\,(f,g) = \frac{(-1)^0}{3^{2+1}} \times (9) = \frac{9}{27} = \frac{1}{3}.$$

Therefore, after the first remainder has been computed, we have $\varrho_1 = \dfrac{5}{9}$, and $p_1 = 2$, in which case $s_1 = 0$ and $\varphi_2 = \lfloor (s_1+1)/2 \rfloor = 0$.

To compute the first non-zero coefficient of the second remainder, that is $\dfrac{117}{25}$, we set $i = 2$, and from (29) we see that the value of the corresponding determinant, $\mathrm{Det}_{2,1}\,(f,g)$, is 65 — since $\mathrm{Det}_{2,0}\,(f,g) = 0$ and, hence, $r_0^{(2)} = 0$. Then, from (9) we have that

$$\varrho_2 = r_1^{(2)} = \frac{(-1)^{\varphi_2}}{\varrho_1^{p_1+1}\varrho_0^{p_0+p_1}} \times \mathrm{Det}_{2,1}\,(f,g) = \frac{(-1)^0}{(\frac{5}{9})^{2+1}3^{2+2}} \times 65 = \frac{117}{25}.$$

The other two coefficients of the second remainder are

$$r_2^{(2)} = \frac{(-1)^{\varphi_2}}{\varrho_1^{p_1+1}\varrho_0^{p_0+p_1}} \times \mathrm{Det}_{2,2}\,(f,g) = \frac{(-1)^0}{(\frac{5}{9})^{2+1}3^{2+2}} \times 125 = 9,$$

and

$$r_3^{(2)} = \frac{(-1)^{\varphi_2}}{\varrho_1^{p_1+1}\varrho_0^{p_0+p_1}} \times \mathrm{Det}_{2,3}\,(f,g) = \frac{(-1)^0}{(\frac{5}{9})^{2+1}3^{2+2}} \times (-245) = -\frac{441}{25}.$$

Therefore, after the second remainder has been computed, we have $\varrho_2 = \dfrac{117}{25}$ and $p_2 = 2$, in which case $s_2 = 0$ and $\varphi_3 = \lfloor (s_2+1)/2 \rfloor = 0$.

To compute the first non-zero coefficient of the third remainder, that is $\dfrac{233150}{19773}$, we set $i = 3$, and from (29) we see that the value of the corresponding determinant, $\mathrm{Det}_{3,0}\,(f,g)$, is 9326. Then, from (9) we have that

$$\varrho_3 = r_0^{(3)} = \frac{(-1)^{\varphi_3}}{\varrho_2^{p_2+1}\varrho_1^{p_1+p_2}\varrho_0^{p_0+p_1}} \times \mathrm{Det}_{3,0}\,(f,g) = \frac{(-1)^0}{(\frac{117}{25})^{2+1}(\frac{5}{9})^{2+2}3^{2+2})} \times 9326 = \frac{233150}{19773},$$

and likewise the last coefficient of the third remainder is

$$r_1^{(3)} = \frac{(-1)^{\varphi_3}}{\varrho_2^{p_2+1}\varrho_1^{p_1+p_2}\varrho_0^{p_0+p_1}} \times \mathrm{Det}_{3,1}\,(f,g) = \frac{(-1)^0}{(\frac{117}{25})^{2+1}(\frac{5}{9})^{2+2}3^{2+2})} \times (-12300) = -\frac{102500}{6591}.$$

Therefore, after the third remainder has been computed, we have $\varrho_3 = \frac{233150}{19773}$ and $p_3 = 1$, in which case $s_3 = 1$ and $\varphi_4 = \lfloor (s_3 + 1)/2 \rfloor = 1$.

To compute the constant term of the fourth remainder, that is $-\frac{1288744821}{543589225}$, we set $i = 4$, and from (29) we see that the value of the corresponding determinant, $\mathrm{Det}_{4,0}(f, g)$, is 260708. Then from (9) we have that

$$\varrho_4 = r_0^{(4)} = \frac{(-1)^{\varphi_4}}{\varrho_3^{p_3+1}\varrho_2^{p_2+p_3}\varrho_1^{p_1+p_2}\varrho_0^{p_0+p_1}} \times \mathrm{Det}_{4,0}(f, g) =$$
$$\frac{(-1)^1}{(\frac{233150}{19773})^{1+1}(\frac{117}{25})^{2+1}(\frac{5}{9})^{2+2}3^{2+2}} \times 260708 = -\frac{1288744821}{543589225}.$$

Thus we have computed all the rational coefficients of the modified Euclidean prs (30). Applying Lemma 1 to the modified Euclidean coefficients we obtain the Euclidean prs

$$(31)\quad x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21,$$
$$-5x^4/9 + x^2/9 - 1/3, -117x^2/25 - 9x + 441/25,$$
$$233150x/19773 - 102500/6591, -1288744821/543589225.$$

Once we have computed the modified Euclidean and Euclidean prs's in $\mathbb{Q}[x]$ with *correct* signs, we can also compute these sequences in $\mathbb{Z}[x]$[6] to obtain, respectively,

$$(32)\quad x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21,$$
$$15x^4 - 3x^2 + 9, 65x^2 + 125x - 245, 9326x - 12300, -260708,$$

and

$$(33)\quad x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21,$$
$$-15x^4 + 3x^2 - 9, -65x^2 - 125x + 245, 9326x - 12300, -260708.$$

Note that in both (32) and (33) the *absolute* values of the coefficients are equal to the *absolute* values of the corresponding coefficients in the subresultant prs (29) of f, g.

Moreover, the sign sequences of (31) and (33) are identical and so are the sign sequences of (30) and (32).

[6] As explained elsewhere, [4], this is achieved by first performing polynomial divisions in $\mathbb{Q}[x]$, in order to compute the correct signs of the remainders. Then, each remainder is computed in $\mathbb{Z}[x]$ by multiplying it times the absolute value of the corresponding denominator of the first fraction in (9) — or in (10).

5. Conclusions. Given the polynomials $f, g \in \mathbb{Z}[\mathbb{x}]$ our main result, Theorem 1, establishes a one-to-one correspondence between the Euclidean and modified Euclidean prs's[7] of f, g, on one hand, and the subresultant prs[8] of f, g, on the other. Therefore, we can *uniquely* compute the *exact* coefficients of the Euclidean and modified Euclidean prs's of f, g from the coefficients of the subresultant prs of f, g, and *vice versa*.

Our work — which improves our earlier work on the subject [5] — complements and extends the work by Pell and Gordon [19]. The terms "modified" Euclidean prs as well "modified" subresultant prs were inspired by the title of their paper.

Acknowledgements. We wish to thank an unknown referee for the very constructive comments, which simplified the proof of our theorem.

REFERENCES

[1] Akritas A. G. A Simple Proof of the Validity of the Reduced PRS Algorithm. *Computing*, **38** (1987), 369–372.

[2] Akritas A. G. Elements of Computer Algebra with Applications. Wiley, 1989.

[3] Akritas A. G., G. I. Malaschonok, P. S. Vigklas. On a Theorem by Van Vleck Regarding Sturm Sequences. *Serdica Journal of Computing*, **7** (2013), No 4, 101–134.

[4] Akritas A. G., G. I. Malaschonok, P. S. Vigklas. Sturm Sequences and Modified Subresultant Polynomial Remainder Sequences. *Serdica Journal of Computing*, **8** (2014), No 1, 29–46.

[5] Akritas A. G., G. I. Malaschonok, P. S. Vigklas. On the Remainders Obtained in Finding the Greatest Common Divisor of Two Polynomials. *Serdica Journal of Computing*, **9** (2015), No 2, 123–138.

[6] Basu S., R. Pollack, M. F. Roy. Algorithms in Real Algebraic Geometry. 2nd Edition, Springer, 2006.

[7] Brown W. S. The subresultant PRS Algorithm. *ACM Transactions on Mathematical Software*, **4** (1978), No 3, 237–249.

[7] Computed either in $\mathbb{Q}[\mathbb{x}]$ or in $\mathbb{Z}[\mathbb{x}]$.

[8] Computed in $\mathbb{Z}[\mathbb{x}]$.

[8] Brown W. S., J. F. Traub. On Euclid's Algorithm and the Theory of Subresultants. *Journal of the Association for Computing Machinery*, **18** (1971), 505–514.

[9] Cohen J. E. Computer Algebra and Symbolic Computation – Mathematical Methods. A. K. Peters, Massachusetts, 2003.

[10] Collins G. E. Polynomial Remainder Sequences and Determinants. *American Mathematical Monthly*, **73** (1966), No 7, 708–712.

[11] Collins G. E. Subresultants and Reduced Polynomial Remainder Sequences. *Journal of the Association for Computing Machinery*, **14** (1967), 128–142.

[12] Diaz–Toca G. M., L. Gonzalez–Vega. Various New Expressions for Subresultants and Their Applications. *Applicable Algebra in Engineering, Communication and Computing*, **15** (2004), 233–266.

[13] Von zur Gathen J., T. Lücking. Subresultants Revisited. *Theoretical Computer Science*, **297** (2003), Issues 1–3, 199–239.

[14] Geddes K. O., S. R. Czapor, G. Labahn. Algorithms For Computer Algebra. Kluwer Academic Publishers, 1992.

[15] Habicht W. Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens. *Commentarii Mathematici Helvetici*, **21** (1948), 99–116.

[16] Iliev A., N. Kyurkchiev. Nontrivial Methods in Numerical Analysis: Selected Topics in Numerical Analysis. LAP LAMBERT Academic Publishing, Saarbrücken, 2010.

[17] Lazard D. Pseudo-remainder sequences. `https://en.wikipedia.org/wiki/Polynomial_greatest_common_divisor#Pseudo-remainder_sequences`, 14 December 2016.

[18] Lombardi H., M.-F. Roy, M. Safey El Din. New structure theorems for subresultants. Special Issue Symbolic Computation in Algebra, Analysis, and Geometry. *Journal of Symbolic Computation*, **29** (2000), 663–690.

[19] Pell A. J., R. L. Gordon. The Modified Remainders Obtained in Finding the Highest Common Factor of Two Polynomials. *Annals of Mathematics*, Second Series, **18** (1917), No 4, 188–193.

[20] Sendov B., A. Andreev, N. Kjurkchiev. Numerical Solution of Polynomial Equations. *Handbook of Numerical Analysis*, **3** (1994), 625–778.

[21] Sylvester, J. J. A method of determining by mere inspection the derivatives from two equations of any degree. *Philosophical Magazine*, **16** (1840), 132–135.

[22] Sylvester J. J. On the Theory of Syzygetic Relations of Two Rational Integral Functions, Comprising an Application to the Theory of Sturm's Functions, and that of the Greatest Algebraical Common Measure. *Philosophical Transactions*, **143** (1853), 407–548.

[23] Sylvester J. J. On a remarkable modification of Sturm's theorem. *Philosophical Magazine and Journal of Science*, **V**, Fourth Series (January–June, 1853), 446–456. `http://books.google.gr/books?hl=el&id=3Ov22-gFMnEC&q=sylvester#v=onepage&q&f=false`, 14 December 2016.

[24] Van Vleck E. B. On the Determination of a Series of Sturm's Functions by the Calculation of a Single Determinant. *Annals of Mathematics*, Second Series, **1** (1899–1900), No 1/4, 1–13.

Alkiviadis G. Akritas
e-mail: `akritas@uth.gr`
Panagiotis S. Vigklas
e-mail: `pviglas@uth.gr`
Department of Electrical and Computer Engineering
University of Thessaly
GR-38221, Volos, Greece

Gennadi I. Malaschonok
Laboratory for Algebraic Computations
Tambov State University
33, Internatsionalnaya
RU-392000 Tambov, Russia
e-mail: `malaschonok@gmail.com`

Received May 08, 2016
Final Accepted June 06, 2016