Bull. Aust. Math. Soc. **79** (2009), 299–302
doi:10.1017/S0004972708001275

COMMON FACTORS OF RESULTANTS MODULO p

DOMINGO GOMEZ, JAIME GUTIERREZ ✉, ÁLVAR IBEAS and DAVID SEVILLA

(Received 16 June 2008)

Abstract

We show that the multiplicity of a prime p as a factor of the resultant of two polynomials with integer coefficients is at least the degree of their greatest common divisor modulo p. This answers an open question by Konyagin and Shparlinski.

2000 *Mathematics subject classification*: primary 13A35; secondary 11C08.
Keywords and phrases: resultant, reduction modulo p.

Given two polynomials

$$F(x) = \sum_{i=0}^{n} \alpha_i x^i \quad \text{and} \quad G(x) = \sum_{i=0}^{m} \beta_i x^i$$

of degree n and m respectively and with integer coefficients, we denote by $S(F, G)$ the Sylvester matrix associated to the polynomials f and g, that is,

$$S(F, G) = \begin{pmatrix} \alpha_0 & & \cdots & & \alpha_n & 0 & \cdots & \cdots & 0 \\ 0 & \alpha_0 & & \cdots & & \alpha_n & 0 & \cdots & 0 \\ \vdots & & \ddots & & & & \ddots & & \\ 0 & \cdots & 0 & \alpha_0 & & \cdots & & \alpha_n & 0 \\ 0 & \cdots & \cdots & 0 & \alpha_0 & & \cdots & & \alpha_n \\ \beta_0 & & \cdots & & \beta_m & 0 & \cdots & \cdots & 0 \\ 0 & \beta_0 & & \cdots & & \beta_m & 0 & \cdots & 0 \\ \vdots & & \ddots & & & & \ddots & & \\ 0 & \cdots & 0 & \beta_0 & & \cdots & & \beta_m & 0 \\ 0 & \cdots & \cdots & 0 & \beta_0 & & \cdots & & \beta_m \end{pmatrix}.$$

We denote by $\mathrm{Res}(F, G)$ the resultant of $F(x)$ and $G(x)$ with respect to x, that is,

$$\mathrm{Res}(F, G) = \det S(F, G),$$

see [2, 3].

This work is partially supported by the Spanish Ministry of Education and Science grant MTM2007-67088.

Let p be a prime. It is well known that if the polynomials F and G have a common factor modulo p then $\mathrm{Res}(F, G) \equiv 0 \bmod p$. It is natural to consider the relation between the multiplicity of p as a factor of $\mathrm{Res}(F, G)$ and the degree of this common factor. In some special case, a positive answer to this question has been given in [1, Lemma 5.3] and the problem of extending this result to the general case has been posed in [1, Question 5.4]. Here we give a full solution to this problem.

Let $FG \not\equiv 0 \bmod p$ and let d_p be the degree of the gcd of the reductions of F and G modulo p. Let r_p be the p-adic order of $\mathrm{Res}(F, G)$. Then the immediate result is

$$d_p > 0 \Rightarrow r_p > 0.$$

The following theorem is our result.

THEOREM. *With the above definitions,*

$$d_p \le r_p.$$

PROOF. We shall prove the following result. Let $H(x)$ be a polynomial of degree t such that its leading coefficient is not a multiple of p. If H divides F and G modulo p, then there exists $\alpha \in \mathbb{Z}$ satisfying

$$\mathrm{Res}(F, G) = \alpha p^t.$$

By the condition on the leading coefficient of H, there exist polynomials

$$f(x) = \sum_{j=0}^{r} b_j x^j \quad \text{and} \quad g(x) = \sum_{i=0}^{s} a_i x^i$$

with $a_s \not\equiv 0 \bmod p$, $r + t \le n$, $s + t \le m$ and satisfying

$$F(x) \equiv H(x) f(x) \bmod p, \qquad G(x) \equiv H(x) g(x) \bmod p.$$

We see that

$$C(x) = F(x)g(x) - G(x)f(x) \equiv 0 \bmod p.$$

We denote by R_i, $i = 1, \ldots, m + n$, the row vectors of $S(F, G)$. Recalling that

$$C(x) = \sum_{i=0}^{s} a_i x^i F(x) - \sum_{j=0}^{r} b_j x^j G(x),$$

we immediately derive that

$$a_s R_{s+1} + \sum_{i=0}^{s-1} a_i R_{i+1} - \sum_{j=0}^{r} b_j R_{m+j+1} \equiv (0, \ldots, 0) \bmod p.$$

Similarly, considering $x^k C(x)$, we obtain

$$a_s R_{s+k+1} + \sum_{i=0}^{s-1} a_i R_{i+k+1} - \sum_{j=0}^{r} b_j R_{m+k+j+1} \equiv (0, \ldots, 0) \bmod p, \tag{1}$$

for $k = 0, \ldots, t - 1$.

We consider the matrix T obtained by replacing the rows $R_{s+1}, \ldots, R_{s+t}$ with the rows $a_s R_{s+1}, \ldots, a_s R_{s+t}$ in $S(F, G)$. Clearly

$$\det T = a_s^t \det S(F, G) = a_s^t \operatorname{Res}(F, G). \tag{2}$$

Using (1) we see that, performing elementary row operations on the matrix T that preserve its determinant, we can obtain a certain matrix whose rows $s+1, \ldots, s+t$ are zero vectors modulo p. Therefore $\det T \equiv 0 \bmod p^t$. Recalling that $a_s \not\equiv 0 \bmod p$, from (2) we conclude the proof. □

The presented proof is also valid for arbitrary unique factorization domains and modulo any principal prime ideal $I = (p)$. In particular, we have the result for any polynomial ring $K[x_1, \ldots, x_n][x]$ modulo an irreducible polynomial $p(x) \in K[x_1, \ldots, x_n][x]$, where K is an arbitrary field.

On the other hand, the naive generalization of the original result, that is, $d_p = r_p$, is clearly false as it suffices to choose two polynomials with a common root. We provide an example that shows that the multiplicity can be strictly higher for pairs of polynomials with no common roots.

EXAMPLE 1. The polynomials $x^2 - 2x$ and $x^2 - 2x + 2$ have no common roots. Let

$$F(x) = x \cdot (x^2 - 2x), \quad G(x) = (x-3)(x^2 - 2x + 2).$$

The greatest common divisor of F and G modulo 3 is x. However,

$$\operatorname{Res}(F, G) = 72 = 3^2 \cdot 8.$$

Finally, the next example shows that $r_p - d_p$ cannot be bounded even if we bound the degrees of F and G.

EXAMPLE 2. For any $p > 2$ and any $k > 0$, let $F = x(x-1)$ and $G = (x - p^k)(x-2)$. Then $d_p = \deg x = 1$ and $r_p \geq k$.

Acknowledgement

The authors would like to thank Igor Shparlinski for his interest and for posing this question.

References

[1] S. V. Konyagin and I. Shparlinski, *Character Sums with Exponential Functions and their Applications* (Cambridge University Press, Cambridge, 1999).
[2] R. Lidl and H. Niederreiter, *Finite Fields* (Cambridge University Press, Cambridge, 1997).
[3] B. L. van der Waerden, *Modern Algebra* (Frederick Ungar Publishing Co., New York, 1964).

DOMINGO GOMEZ, University of Cantabria, E-39071 Santander, Spain
e-mail: domingo.gomez@unican.es

JAIME GUTIERREZ, University of Cantabria, E-39071 Santander, Spain
e-mail: jaime.gutierrez@unican.es

ÁLVAR IBEAS, University of Cantabria, E-39071 Santander, Spain
e-mail: alvar.ibeas@unican.es

DAVID SEVILLA, Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, Altenbergerstraße 69, A-4040 Linz, Austria
e-mail: david.sevilla@oeaw.ac.at