Bull. Math. Soc. Sc. Math. Roumanie
Tome 49(97) No. 1, 2006, 69–74

Polynomial Factorizations

by
Laurenţiu Panaitopol and Doru Ştefănescu *

To Professor Ion D. Ion on the occasion of his 70th Birthday

Abstract

In this paper we describe necessary conditions for the factorization of polynomials from $\mathbb{Z}[X]$ which can be represented as $f_1 f_2 + pg$, with p a convenient prime number. These conditions are derived using resultants. This approach allows us to construct irreducible polynomials.

Key Words: Factorization of polynomials, irreducible polynomials.
2000 Mathematics Subject Classification: Primary: 12D05, Secondary 11T06.

We consider the family of polynomials with integer coefficients

$$F = f_1 f_2 + pg,$$

where F, f_1, f_2 are supposed monic and $p > 2$ is prime.

We describe factorization conditions for such polynomials, expressed in terms of resultants. These conditions are then applied to the construction of classes of irreducible polynomials.

Throughout this paper $R(f, g)$ will denote the resultant of the polynomials f and g. If $f(X) = \sum_{j=0}^{d} a_j X^j \in \mathbb{Z}[X]$ and $p \geq 2$ is prime, we denote by $\overline{f}$ the polynomial $\overline{f}(X) = \sum_{j=0}^{d} \overline{a}_j X^j \in \mathbb{Z}_p[X]$, where $\overline{a}_j$ is the image of a_j in $\mathbb{Z}_p$.

Proposition 1. *Let $F(X) = f_1(X) f_2(X) + pg(X) \in \mathbb{Z}[X]$ be a monic polynomial. Let us suppose that f_1, f_2 are monic, $\overline{f}_1, \overline{f}_2$ are irreducible in $\mathbb{Z}_p[X]$, $\overline{f_1} \neq \overline{f_2}$ and p is a prime number.*

If F is reducible in $\mathbb{Z}[X]$ we have:

i. There exists a divisor $b \in \mathbb{Z}$ of $R(F, g)$ such that $R(f_1, f_2)^2 \equiv b \bmod p$.

ii. There exist $a_1, a_2 \in \mathbb{Z}$ such that $a_1 a_2 \mid R(F, g)$ and

$$a_1 \equiv a_2 \equiv R(f_1, f_2) \bmod p.$$

*The second author was partially supported by grant CEx05-D11-03 during this research.

Proof: Since F, f_1 and f_2 are monic, we have $\deg(g) < \deg(F)$.
Let's suppose that there exist $F_1, F_2 \in \mathbb{Z}[X] \setminus \mathbb{Z}$ such that

$$F = F_1 F_2.$$

Then F_1 and F_2 are monic. Since $\overline{f}_1$ and $\overline{f}_2$ are irreducible in $\mathbb{Z}_p$ we have

$$F_1 = f_1 + pg_1, \quad F_2 = f_2 + pg_2, \tag{1}$$

with $\deg(g_1) < \deg(F_1)$, $\deg(g_2) < \deg(F_2)$.
It follows that

$$g = f_1 g_2 + f_2 g_1 + p g_1 g_2. \tag{2}$$

We consider now the resultants of the polynomial f_1, respectively f_2 with the polynomial g. From (2) it follows that

$$\begin{cases} R(f_1, g) = R(f_1, g_1) R(f_1, f_2 + pg_2), \\ \\ R(f_2, g) = R(f_2, g_2) R(f_2, f_1 + pg_1). \end{cases} \tag{3}$$

Therefore there exist $u_1, u_2 \in \mathbb{Z}$ such that

$$\begin{cases} R(f_1, g) = R(f_1, g_1)[R(f_1, f_2) + pu_1], \\ \\ R(f_2, g) = R(f_2, g_2)[R(f_2, f_1) + pu_2]. \end{cases} \tag{4}$$

Now we multiply the two relations from (4). Because

$$R(F, g) = R(f_1 f_2 + pg, g) = R(f_1 f_2, g) = R(f_1, g) R(f_2, g)$$

it follows that

$$\varepsilon\, R(f_1, f_2)^2 + p(\varepsilon\, u_1 + u_2) R(f_1, f_2) + p^2 u_1 u_2 \;=\; a\,, \tag{5}$$

where $\varepsilon = (-1)^{\deg(f_1)\deg(f_2)}$ and a is a divisor of the integer number $R(F, g)$. We put $b = \varepsilon\, a$ and (5) proves *i*.

From (3) we obtain

$$\begin{cases} R(f_1, g) \;= a_1\, R(f_1, g_1) \\ \\ R(f_2, g) \;= \varepsilon\, a_2\, R(f_2, g_2)\,, \end{cases} \tag{6}$$

with $a_1 = R(f_1, f_2 + pg_2)$, $a_2 = R(f_1 + pg_1, f_2)$.

We have $a_2 = \varepsilon\, R(f_2, f_1 + pg_1)$. Therefeore

$$a_1 \;\equiv\; a_2 \;\equiv\; R(f_1, f_2) \mod p$$

and, by (6),

$$R(F, g) \;=\; R(f_1 f_2, g) \;=\; \varepsilon\, a_1 a_2 R(f_1, g_1) R(f_2, g_2)\,,$$

which proves *ii*. □

Theorem 1. *Let $F(X) = f_1(X)f_2(X) + pg(X) \in \mathbb{Z}[X]$ be a monic polynomial. Suppose that f_1, f_2 are monic, $\overline{f}_1, \overline{f}_2$ are irreducible in $\mathbb{Z}_p[X]$, $\overline{f_1} \neq \overline{f_2}$, $R(F,g) \neq 0$ and square-free, and p is a prime number such that $p > 2|R(F,g)|$.*

If F is reducible in $\mathbb{Z}[X]$ then

$$R(f_1, f_2) \equiv \pm 1 \bmod p\,. \tag{7}$$

Proof: From relation (5) in the proof of Proposition 1 we have

$$\varepsilon\, R(f_1,f_2)^2 + p(\varepsilon\, u_1 + u_2)R(f_1,f_2) + p^2 u_1 u_2 \;=\; a\,, \tag{8}$$

where a is a divisor of the nonzero integer $R(F,g)$.

From (8) it follows that $R(f_1,f_2)$ is an integer solution of the quadratic equation

$$\varepsilon\, y^2 + p(\varepsilon\, u_1 + u_2)y + p^2 u_1 u_2 - a = 0. \tag{9}$$

Therefore the discriminant of (9) must be a perfect square. Hence there exists $t \in \mathbb{Z}$ such that

$$p^2(\varepsilon\, u_1 + u_2)^2 - 4\varepsilon\, p^2 u_1 u_2 + 4\varepsilon\, a = p^2(\varepsilon\, u_1 - u_2)^2 + 4\varepsilon\, a = t^2. \tag{10}$$

Denoting $\varepsilon u_1 - u_2$ by x, we have

$$p^2 x^2 + 4\varepsilon\, a = t^2,$$

that is

$$4\varepsilon\, a = t^2 - (px)^2. \tag{11}$$

Since $p > 2|R(F,g)|$ we have $p > 2$ and it follows that the following relation holds in $\mathbb{Z}_p$:

$$\overline{\varepsilon\, a} = (\overline{2}^{-1}\overline{t})^2, \tag{12}$$

i.e. $\varepsilon\, a$ is a quadratic residue modulo p.

The numbers $t - px$ and $t + px$ have the same parity and from (11) it follows that they are even. Since

$$|a| \;=\; |\varepsilon\, a| \;=\; \left|\frac{t-px}{2}\right| \cdot \left|\frac{t+px}{2}\right|,$$

we have

$$\frac{|t| + |px|}{2} \;\leq\; |a|\,.$$

Hence

$$p|x| \;\leq\; |t| + p|x| \;\leq\; 2|a|\,.$$

Since a is a divisor of $R(F,g)$ and $p > 2|R(F,g)|$ we have $p > 2|a|$. But for nonzero x we have $p \leq |px| \leq 2|a|$. Therefore $x = 0$ and from relation (11) we

deduce that $4\varepsilon\, a = t^2$. But $R(F,g)$ is square-free, so $\varepsilon\, a = 1$. Therefore from (8) we deduce that

$$R(f_1,f_2)^2 + p(u_1 + \varepsilon\, u_2)R(f_1,f_2) + \varepsilon\, p^2 u_1 u_2 \;=\; 1\,,$$

hence

$$R(f_1,f_2)^2 + pk \;=\; 1\,, \quad \text{with} \quad k \in \mathbb{Z}\,,$$

which proves that

$$R(f_1,f_2) \;\equiv\; \pm 1 \mod p\,.$$

□

Example 1. *Let $F(X) = X^4 + X^2 + 1 + p(X^2-1)$, with p a prime of the form $3k+2$, $p \geq 11$.*

We have $F = f_1 f_2 + pg$, with

$$f_1(X) = X^2 + X + 1\,, \quad f_2(X) = X^2 - X + 1\,, \quad g(X) = X^2 - 1\,.$$

Since $p \equiv 2 \mod 3$, the polynomials $\overline{f}_1$ and $\overline{f}_2$ are irreducible in $\mathbb{Z}_p[X]$.

By Proposition 1 there exist integers a_1, a_2 whose product divides 9 (which is the resultant of F and g) and such that

$$a_1 \;\equiv\; a_2 \equiv R(f_1,f_2) = 4 \mod p\,.$$

Since $a_1 a_2$ divides 9 and $p \geq 11$ we have

$$a_1 \;= a_2 \;\in\; \{\pm 1, \pm 3\}\,.$$

Therefore p divides $R(f_1,f_2) - a_1 = 4 - a_1$ and we obtain

$$p \in \{3,5,7\}\,.$$

But $p \equiv 2 \mod 3$, so $p = 5$. Since $p \geq 11$ it follows that the polynomial $F(X) = X^4 + X^2 + 1 + p(X^2-1)$ is irreducible in $\mathbb{Z}[X]$. We observe that also $X^4 + X^2 + 1 + 5(X^2-1) = X^4 + 6X^2 - 4$ is irreducible in $\mathbb{Z}[X]$.

Note that the polynomial F is not a Schönemann polynomial (cf. [2]).

Example 2. *Let $F(X) = X^4 + (p+2)X^3 + 3X^2 + 2X + 2$, with p a prime integer, $p = 4k+3$, $p > 23$.*

We consider $f_1(X) = X^2 + 1$, $f_2(X) = (X+1)^2 + 1$, $g(X) = X^3$. We have $F(X) = (X^2+1)(X^2+2X+2) + pX^3$, $R(F,g) = 8$, and $R(f_1,f_2) = 5$.

Since $p \equiv 3 \mod 4$, the polynomials $\overline{f}_1$ and $\overline{f}_2$ are irreducible in $\mathbb{Z}_p[X]$. By Proposition 1 there exists a divisor a of $8 = R(F,g)$ such that $25 = R(f_1,f_2)^2 \equiv a \mod p$. It follows that p divides one of the numbers

$$25-1\,,25+1\,,25-2\,,25+2\,,25-4\,,25+4\,,25-8\,,25+8\,.$$

Since $p > 23$, it follows that $p = 29$. But this value of p is inconvenient because 29 is not of the form $4k+3$. It follows that F is irreducible in $\mathbb{Z}[X]$.

Corollary 1. *The polynomials* $X^4+4+p(X+1)$ *and* $X^4+4+p(X-1)$ *are irreducible in* $\mathbb{Z}[X]$ *for any prime* p *of the form* $4k+3$.

Proof: We consider $F(X)=X^4+4+p(X\pm 1)$, with p prime, $p\geq 11$. We have

$$X^4+4 \;=\; (X^2+2X+2)(X^2-2X+2)\,,$$

so we put

$$f_1(X) \;=\; (X+1)^2+1, \quad f_2(X) \;=\; (X-1)^2+1\,.$$

and

$$g(X) \;=\; X+1 \quad \text{or} \quad X-1\,.$$

Since p is of the form $4k+3$, the polynomials $\overline{f}_1$ and $\overline{f}_2$ are irreducible in $\mathbb{Z}_p[X]$.

We have $R(F,g)=5$ and $R(f_1,f_2)=32$. By Theorem 1 we have $32=\pm 1 \bmod p$. Therefore p divides 32 ± 1, so $p\in\{3,11,31\}$. Since $p\geq 11$, we have $p\in\{11,31\}$. The corresponding polynomials are

$$X^4+11X-7\,, \qquad X^4+11X+15\,,$$

$$X^4+31X-27\,, \quad X^4+31X+35\,.$$

By direct verification it follows that they are irreducible in $\mathbb{Z}[X]$.
If $p<10$ we have $p=3$ or $p=7$. The corresponding polynomials

$$X^4+3X+1\,, \quad X^4+3X+7\,,$$

$$X^4+7X-3\,, \quad X^4+7X+11$$

are also irreducible in $\mathbb{Z}[X]$. □

With the notation and assumptions of Proposition 1 and of Theorem 1 we can now derive the following results.

Corollary 2. *Let* $f_1,f_2\in\mathbb{Z}[X]$ *be monic and such that* $R(f_1,f_2)\not\equiv\pm 1 \bmod p$. *If* $g\in\mathbb{Z}[X]$ *and* $\deg(g)<\deg(f_1f_2)$, *then the polynomial* $F=f_1f_2+pg$ *is irreducible in* $\mathbb{Z}[X]$.

Corollary 3. *If* $R(F,g)\neq 0$ *and has not two factors of the form* $\mathcal{M}p+R(f_1,f_2)$, *then the polynomial* F *is irreducible in* $\mathbb{Z}[X]$.

Proof: If F is reducible it follows from Proposition 1 that there exist integers a_1,a_2 such that

$$a_1a_2 \mid R(F,g), \qquad a_1=\mathcal{M}p\pm R(f_1,f_2), \qquad a_2=\mathcal{M}p\pm R(f_1,f_2)\,.$$

□

Acknowledgement: We warmly thank Mihai Cipu for fruitful comments and suggestions concerning this work.

References

[1] L. Panaitopol, D. Ştefănescu: A Resultant Condition for the Irreducibility of the Polynomials, *J. Number Theory*, **25**, 107–111 (1987).

[2] L. Panaitopol, D. Ştefănescu: Factorization of the Schönemann polynomials, *Bull. Math. Soc. Sci. Math. Roumanie*, **32 (80)**, 259–262 (1988).

[3] V. V. Prasolov: *Polynomials*, Springer Verlag, Berlin (2004).

Received: 7.12.2005

University of Bucharest
Faculty of Mathematics
Str. Academiei 14
Bucharest, Romania
E-mail: pan@al.math.unibuc.ro

University of Buhcarest
Faculty of Physics
Department of Mathematics
P. O. Box 39-D5
Bucharest 39, Romania
E-mail: stef@rms.unibuc.ro