sciendo

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.2478/tmmp-2023-0001
Tatra Mt. Math. Publ. **83** (2023), 1–10

IRREDUCIBILITY AND MULTIPLICATIVE COMPOSITION OF POLYNOMIALS OVER FINITE FIELDS

Leila Benferhat [1] — Omar Kihel[2] — Jesse Larone[2] — Rezki Ould Mohamed[3]

[1]National Higher School of Artificial Intelligence, Mahelma, ALGERIA

[2]Brock University, St. Catharines, CANADA

[3]University of Science and Technology Houari Boumediene, Algiers, ALGERIA

ABSTRACT. The aim of this paper is to provide integral polynomials irreducible over $\mathbb{Z}$ which are reducible over $\mathbb{F}_p$ for every prime p. In particular, we show that certain composed products of integral polynomials are reducible modulo p for all primes p.

1. Introduction

Let $f, g \in \mathbb{F}_q[x]$ be two monic polynomials over the finite field of q elements. Brawley and Carlitz [3] studied various forms of composed products of the two polynomials, denoted by $f \diamond g$. Among them are the composed products induced by the field multiplication and field addition on the algebraic closure of $\mathbb{F}_q$. In particular, let $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ be all the roots of f and g, respectively, in an algebraic closure of $\mathbb{F}_q$. The composed addition of f and g is given by

$$\prod_{i=1}^{m}\prod_{j=1}^{n}\left(x-(\alpha_i+\beta_j)\right),$$

and the composed multiplication of f and g is given by

$$\prod_{i=1}^{m}\prod_{j=1}^{n}(x-\alpha_i\beta_j).$$

Among other results, they prove the following theorem

2020 Mathematics Subject Classification: 11T06, 13F15, 11C08.
Keywords: polynomial, polynomial decomposition, resultant .
[3]The corresponding author.

Theorem 1.1. *Let $f, g \in \mathbb{F}_q[x]$ be monic polynomials with $\deg f = m$ and $\deg g = n$. Then $f \diamond g$ is irreducible if and only if both f and g are irreducible and $\gcd(m, n) = 1$.*

The majority of the remaining results from their paper deal with decomposing polynomials and the properties of such decompositions.

The additive decomposition of polynomials over unique factorization domains has been studied in [2].

In this paper, using composed multiplication, we provide additional integral polynomials irreducible over $\mathbb{Z}$ which are reducible over $\mathbb{F}_p$ for every prime p. Let R be a commutative ring. We recall that the resultant of two polynomials $f, g \in R[x]$, denoted by $\mathrm{Res}_x(f, g)$, is the determinant of their Sylvester matrix. In [1], Ayad shows that if the monic polynomials $f, g \in \mathbb{Z}[x]$ satisfy certain additional properties, then the polynomial

$$\mathrm{Res}_y\big(f(y), g(x - y)\big) \in \mathbb{Z}[x]$$

is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{F}_p$ for all primes p. This polynomial is related to the composed addition of f and g by

$$\prod_{i=1}^{m} \prod_{j=1}^{n} \big(x - (\alpha_i + \beta_j)\big) = \mathrm{Res}_y\big(f(y), g(x - y)\big),$$

where $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ are all the roots of f and of g, respectively, in $\mathbb{C}$.

2. Preliminaries

Throughout the paper, let R and S denote two integral domains. Consider

$$g = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0 \in R[x] \quad \text{with} \quad b_n \neq 0.$$

The homogenization of g, denoted ${}^h g(y, x)$, is the polynomial defined by

$${}^h g(y, x) := b_n x^n + b_{n-1} x^{n-1} y + \cdots + b_1 x y^{n-1} + b_0 y^n.$$

It is a homogeneous polynomial in $R[x, y]$ of degree $n = \deg g$ such that

$${}^h g(1, x) = g(x).$$

Direct comparison shows that

$$y^n g(x/y) = b_n x^n + b_{n-1} x^{n-1} y + \cdots + b_1 x y^{n-1} + b_0 y^n = {}^h g(y, x)\,.$$

If $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ are all the roots of f and g, respectively, in an algebraic closure of the field of fractions of R, and if C_f and C_g are the respective leading coefficients of f and g, then we obtain

$$\begin{aligned} C_f^n C_g^m \prod_{i=1}^{m}\prod_{j=1}^{n}(x-\alpha_i\beta_j) &= C_f^n \prod_{i=1}^{m}\left(\alpha_i^n C_g \prod_{j=1}^{n}\big(x/\alpha_i-\beta_j\big)\right) \\ &= C_f^n \prod_{i=1}^{m}\big(\alpha_i^n g(x/\alpha_i)\big) \\ &= \mathrm{Res}_y\big(f(y), y^n g(x/y)\big) \\ &= \mathrm{Res}_y\big(f(y), {}^h g(y,x)\big)\,. \end{aligned}$$

This motivates the following proposition

Proposition 2.1. *Let $f, g \in R[x]$. The composed product of f and g is given by*

$$(f \diamond g)(x) = Res_y\big(f(y), {}^h g(y,x)\big).$$

The composed product is an associative and commutative binary operation on $R[x]$. This is routinely verified by considering the roots of polynomials in a given algebraic closure of the field of fractions of R. The operation then inherits commutativity from the commutativity of the products of roots in the algebraic closure. Associativity follows from both $f \diamond (g \diamond h)$ and $(f \diamond g) \diamond h$ being equal to

$$C_f^{\deg g \deg h} C_g^{\deg f \deg h} C_h^{\deg f \deg g} \prod_{\alpha,\beta,\gamma}(x-\alpha\beta\gamma),$$

where the α, β, and γ run over all roots of f, g, and h respectively. It is clear from the definition that if $f = f_1 \diamond f_2$, then

$$C_f = C_{f_1}^{\deg f_2} \cdot C_{f_2}^{\deg f_1}.$$

This property is paralleled with the constant terms of the polynomials. Indeed, let

$$g = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in R[x]$$

and let $f \in R[x]$ be of degree m. If $b_0 \neq 0$, then

$$\begin{aligned} (f \diamond g)(0) &= \mathrm{Res}_y\big(f(y), {}^h g(y,0)\big) \\ &= \mathrm{Res}_y\big(f(y), b_0 y^n\big) \\ &= (-1)^{mn}\mathrm{Res}_y\big(b_0 y^n, f(y)\big) \\ &= (-1)^{mn} b_0^m f(0)^n, \end{aligned}$$

and if $b_0 = 0$, then

$$(f \diamond g)(0) = \mathrm{Res}_y\big(f(y), {}^h g(y,0)\big) = \mathrm{Res}_y\big(f(y), 0\big) = 0\,.$$

Thus,

$$(f \diamond g)(0) = (-1)^{mn} f(0)^n g(0)^m.$$

The set $R[x]$ is closed under the composed product binary operation. It is of interest then to determine the units, if any, with respect to this operation. The polynomial $\ell := x - 1 \in R[x]$ is the identity under $\diamond$. Indeed, for any $f \in R[x]$, we have

$$(\ell \diamond f)(x) = \mathrm{Res}_y\big(\ell(y), {}^h f(y,x)\big) = {}^h f(1,x) = f(x)$$

and

$$(f \diamond \ell)(x) = \mathrm{Res}_y\big(f(y), x - y\big) = (-1)^{2\deg f} \mathrm{Res}_y\big(y - x, f(y)\big) = f(x)\,.$$

If $u, v \in R[x]$ are inverses of one another, then

$$1 = \deg \ell = \deg(u \diamond v) = \deg u \cdot \deg v$$

so that $\deg u = \deg v = 1$. Let $u = u_1 x + u_0$ and $v = v_1 x + v_0$. We have

$$x - 1 = \ell(x) = (u \diamond v)(x) = u_1 v_1 x - u_0 v_0\,,$$

from which we obtain $u_1 v_1 = u_0 v_0 = 1$. That is, u_1 and u_0 are units, and $v = {u_1}^{-1} x + {u_0}^{-1}$. As the composed product is associative on $R[x]$, it is also associative on the subset of linear polynomials. So, we summarize as follows

Theorem 2.2. *The group $G_\diamond$ of units of $R[x]$ under $\diamond$ consists exactly of the linear polynomials $u = u_1 x + u_0$ with $u_1, u_0 \in R^\times$, and the inverse of any such u is given by ${u_1}^{-1} x + {u_0}^{-1}$.*

Proposition 2.3. *Let $G_\diamond$ be the group of units of $R[x]$ under $\diamond$. Then*

$$G_\diamond \simeq R^\times \oplus R^\times.$$

Proof. Let $(\overline{R}, +, *)$ be induced from the ring $(R, +, \cdot)$ with multiplication instead defined by $x * y := -(x \cdot y)$. The map $\phi : R \to \overline{R}$ defined by $\phi(x) = -x$ is a ring isomorphism. Since $R \simeq \overline{R}$ as rings, we obtain $R^\times \simeq \overline{R}^\times$ as groups. Defining the map $\psi : G_\diamond \to R^\times \oplus \overline{R}^\times$ by $\psi(u_1 x + u_0) = (u_1, u_0)$, we have $G_\diamond \simeq R^\times \oplus \overline{R}^\times \simeq R^\times \oplus R^\times$. □

Definition 2.4. Let $f \in R[x]$. If there exist $f_1, f_2 \in R[x] \setminus G_\diamond$ such that $f = f_1 \diamond f_2$, then we say that f is *multiplicatively decomposable*. Otherwise, we say that f is *multiplicatively indecomposable*. If f only admits decompositions of the form $f = f_1 \diamond f_2$ with either f_1 or f_2 linear, then we will say that f is *nearly indecomposable* over R.

3. Indecomposable polynomials

The nearly indecomposable polynomials will be sufficient for the purposes of this paper, but we make here a few comments about indecomposable polynomials. Every indecomposable polynomial is nearly indecomposable by definition, and the two notions coincide over a field. When applicable, the following results can be used to determine when certain nearly indecomposable polynomials are indecomposable.

Lemma 3.1. *Let $f \in R[x]$ be nearly indecomposable over R. If the leading coefficient and constant term of f both lie in $R^\times$, then f is indecomposable over R.*

P r o o f. We have that f is nearly indecomposable, so we write $f = f_1 \diamond f_2$ with f_1 linear without loss of generality. If the leading coefficient C_f of f and $f(0)$ both lie in $R^\times$, then

$$C_f = C_{f_1}^n C_{f_2}$$

and

$$f(0) = (f_1 \diamond f_2)(0) = (-1)^n f_1(0)^n f_2(0)$$

show that $C_{f_1}, f_1(0) \in R^\times$ as well. Thus $f_1 = C_{f_1} x + f_1(0) \in G$, so f is indecomposable. □

Theorem 3.2. *Let $f \in R[x]$ with $\deg f = n \geq 1$. Suppose that $f(0) \in R^\times$ and C_f is prime. If f is nearly indecomposable over R, then f is indecomposable over R.*

P r o o f. Suppose that f is nearly indecomposable. Writing $f = f_1 \diamond f_2$ for some $f_1, f_2 \in R[x]$, we may assume without loss of generality that f_1 linear and f_2 is of degree n. We have

$$f(0) = (f_1 \diamond f_2)(0) = (-1)^n f_1(0)^n f_2(0)\,.$$

As $f(0)$ is a unit, $f_1(0)$ is a unit, and as C_f is prime, C_f is irreducible. From $C_f = C_{f_1}^n C_{f_2}$, we deduce that C_{f_1} or C_{f_2} is a unit.

If C_{f_1} is a unit, then f is indecomposable as $f_1(0)$ is also a unit. If C_{f_2} is a unit, then $C_{f_1}^n = C_f C_{f_2}^{-1}$ implies that C_f divides C_{f_1}. Put $C_{f_1} = C_f \alpha$, $\alpha \in R$, so we have

$$(C_f \alpha)^n C_{f_2} = C_f,$$

and then $C_f^{n-1} \alpha^n C_{f_2} = 1$. In the case $n \geq 2$, we deduce that $C_f \alpha$ is a unit, so that C_{f_1} is as well, and f is indecomposable. In the case $n = 1$, we deduce that C_{f_2} is a unit, and as $f_2(0)$ is also unit, we conclude that f is again indecomposable. □

4. Nearly indecomposable polynomials

We begin this section by presenting two classes of nearly indecomposable polynomials.

Theorem 4.1. *If $f \in R[x]$ has degree p a prime, then f is nearly indecomposable over R.*

Proof. Suppose that $f = f_1 \diamond f_2$ for some $f_1, f_2 \in R[x]$ of degrees m and n, respectively. Since $p = \deg f = mn$, it follows that either f_1 or f_2 is linear. □

Theorem 4.2. *If $f \in R[x]$ with $\deg f > 1$ has leading coefficient p a prime, then f is nearly indecomposable over R. Moreover, the leading coefficient of any linear decomposition factor lies in $R^\times$.*

Proof. Suppose that $f = f_1 \diamond f_2$ for some $f_1, f_2 \in R[x]$ with respective degrees m and n. We have $p = C_{f_1}^n C_{f_2}^m$. Suppose without loss of generality that p divides $C_{f_1}^n$. Then p divides C_{f_1}, and writing $C_{f_1} = pa$ with $a \in R$ yields $p = p^n a^n C_{f_2}^m$, so $0 = p(p^{n-1}a^n C_{f_2}^m - 1)$ implies that $p^{n-1}a^n C_{f_2}^m = 1$. Then p^{n-1} divides 1, which is impossible unless $n = 1$. We conclude that $\deg f_2 = 1$ and $aC_{f_2}^m = 1$. □

Note that if a polynomial $f \in R[x]$ is nearly indecomposable and written as $f = f_1 \diamond \cdots \diamond f_r$, then at most one composition factor is not linear. Indeed, if there are at least two non-linear polynomials f_i and f_j among the composition factors, then we can write $f = f_i \diamond (f_j \diamond g)$ with g being the composition of any remaining composition factors. This would contradict f being nearly indecomposable.

If a polynomial is not nearly indecomposable, then one might ask about a possible decomposition into some nearly indecomposables.

Theorem 4.3. *Let $f \in R[x]$. Then $f = f_1 \diamond f_2 \diamond \cdots \diamond f_r$ for some nearly indecomposable polynomials $f_i \in R[x]$.*

Proof. The case where f is itself indecomposable is trivial. Let us then suppose that f is decomposable and proceed by induction on the degree of f. Since every linear polynomial is nearly indecomposable, the result clearly holds when $\deg f = 1$, so we assume as induction hypothesis that the result also holds for all polynomials of degree less than or equal to the degree of f.

Since f is assumed decomposable, we may write $f = f_1 \diamond f_2$ for some $f_1, f_2 \in R[x] \setminus G_\diamond$. If it is only possible to write $f = f_1 \diamond f_2$ with either f_1 or f_2 linear, then f is nearly indecomposable by definition. If we have a decomposition in which $\deg f_1 < \deg f$ and $\deg f_2 < \deg f$, then by hypothesis $f_1 = g_1 \diamond \cdots \diamond g_t$ and $f_2 = g_{t+1} \diamond g_r$ for some nearly indecomposable polynomials $g_i \in R[x]$. Then $f = g_1 \diamond \cdots \diamond g_r$ as required. □

A ring homomorphism $\sigma : R \to S$ can be naturally extended to a ring homomorphism from $R[x]$ to $S[x]$ by $a_m x^m + \cdots + a_0 \mapsto \sigma(a_m)x^m + \cdots + \sigma(a_0)$. If $\sigma : R[x] \to S[x]$ preserves the degrees of $f, g \in R[x]$, then

$$\sigma\big(\mathrm{Res}_x(f,g)\big) = \mathrm{Res}_x(\sigma f, \sigma g)$$

since $\mathrm{Res}_x(f,g)$ is a polynomial in the coefficients of f and of g. This leads us to the following result

Theorem 4.4. *Let $\sigma : R \to S$ be a ring homomorphism, and let $f \in R[x]$ be such that $f(0), C_f \notin \ker\sigma$. If $f = f_1 \diamond f_2$ over R, then $\sigma f = \sigma f_1 \diamond \sigma f_2$ over S. Moreover, $\deg \sigma f_1 = \deg f_1$ and $\deg \sigma f_2 = \deg f_2$.*

Proof. We naturally extend σ to a ring homomorphism from $R[x,y]$ to $S[x,y]$. By assumption, σ does not map C_f nor $f(0)$ to zero. Denote the respective degrees of f_1 and f_2 by m and n. Then $C_f = C_{f_1}^n C_{f_2}^m$ implies that

$$0 \neq \sigma(C_f) = \sigma(C_{f_1})^n \sigma(C_{f_2})^m,$$

while $f(0) = (-1)^{mn} f_1(0)^n f_2(0)^m$ implies that

$$0 \neq \sigma\big(f_1(0)\big)^n \sigma\big(f_2(0)\big)^n.$$

Since σ does not map the leading coefficients nor the constant terms of f_1 and f_2 to zero, it preserves the degrees of these two polynomials as well as those of ${}^h f_1(y,x)$ and ${}^h f_2(y,x)$. Thus,

$$\sigma(f_1 \diamond f_2) = \sigma\Big(\mathrm{Res}_y\big(f_1(y), {}^h f_2(y,x)\big)\Big) = \mathrm{Res}_y\big(\sigma f_1(y), {}^h \sigma f_2(y,x)\big) = \sigma f_1 \diamond \sigma f_2.$$

□

Theorem 4.5. *Let $\sigma : R \to S$ be a ring homomorphism, and let $f \in R[x]$ be such that $f(0), C_f \notin \ker\sigma$. If σf is nearly indecomposable over S, then f is nearly indecomposable over R.*

Proof. By Theorem 4.3, we write $f = f_1 \diamond \cdots \diamond f_r$, where each $f_i \in R[x]$ is nearly indecomposable over R. Then $\sigma f = \sigma f_1 \diamond \cdots \diamond \sigma f_r$ is nearly indecomposable over S, so all but one of the σf_i are linear, say f_t with $t \in \{1, \ldots, r\}$. It follows from $\deg f_i = \deg \sigma f_i = 1$ that f_i is linear for each $i \in \{1, \ldots, r\} \setminus \{t\}$. Setting $\ell_1 := f_1 \diamond \cdots \diamond f_{t-1}$ and $\ell_2 := f_{t+1} \diamond \cdots \diamond f_r$ yields $f = \ell_1 \diamond f_1 \diamond \ell_2$. Thus, f is nearly indecomposable. □

The proof of the main result requires a lemma, which follows immediately from the definition of composed multiplication:

Lemma 4.6. *Let K be the field of fractions of the integral domain R. Let $f, f_1, f_2 \in R[x]$ and let $f = C_f F$, $f_1 = C_{f_1} F_1$, and $f_2 = C_{f_2} F_2$, where $C_f, C_{f_1}, C_{f_2} \in R$ and $F, F_1, F_2 \in K[x]$ are monic. Then $f = f_1 \diamond f_2$ over R if and only if $F = F_1 \diamond F_2$ over K and $C_f = C_{f_1}^{\deg f_2} C_{f_2}^{\deg f_1}$.*

5. Main result

Theorem 5.1. *Let $\mathfrak{m}$ be a maximal ideal of R such that the residue field $R/\mathfrak{m}$ is finite, and let $f \in R[x]$ be a polynomial of degree at least 2 whose leading coefficient and constant term do not lie in $\mathfrak{m}$. If the image of f modulo $\mathfrak{m}$ is irreducible over $R/\mathfrak{m}$, then f is the multiplicative composition of at most $\omega(\deg f)$ nearly indecomposable polynomials of degrees at least 2 over R, with $\omega(n)$ being the number of primes appearing in the unique factorization of the integer n.*

Proof. Suppose that $f = f_1 \diamond \cdots \diamond f_r$ where each $f_i \in R[x]$ is nearly indecomposable of degree at least 2 over R. Define $\sigma : R \to R/\mathfrak{m}$ by $a \mapsto a \pmod{\mathfrak{m}}$ and extend it to a polynomial ring homomorphism.

Suppose that $r > \omega(\deg f)$. The leading coefficient and constant term of f are not zero modulo $\mathfrak{m}$, so each $\deg f_i = \deg \sigma f_i$ divides $\deg f = \deg \sigma f$ by Theorem 4.5. It follows from the pigeonhole principle that at least two of the $\deg \sigma f_i$ share a prime factor of $\deg \sigma f$, say $\deg \sigma f_1$ and $\deg \sigma f_2$ without loss of generality. Set $\sigma g := \sigma f_2 \diamond \cdots \diamond \sigma f_r$ so that $\sigma f = \sigma f_1 \diamond \sigma g$.

We assume that the polynomials σf_1 and σg are monic, otherwise we simply divide by their leading coefficients and the relationship remains by Lemma 4.6. By assumption, σf is irreducible over $R/\mathfrak{m}$, so we must have $\gcd(\deg \sigma f_1, \deg \sigma g) = 1$ by Theorem 1.1, which contradicts the two degrees sharing a prime factor. Thus, we conclude that $r \leq \omega(\deg f)$. □

Corollary 5.2. *Let $f_1, f_2, \ldots, f_r \in \mathbb{Z}[x]$ all have degrees at least 2. If*

$$\omega(\deg f_1 \cdots \deg f_r) < r\,,$$

then $f_1 \diamond \cdots \diamond f_r$ is reducible modulo p for all primes p not dividing its leading coefficient and constant term.

Proof. For each $i \in \{1, \ldots, r\}$, we decompose the composition factor f_i in the form $f_i = f_{i,1} \diamond \cdots \diamond f_{i,k_i}$ for some $k_i \geq 1$, where $f_{i,j}$ is a nearly indecomposable polynomial of degree at least 2 for each $j \in \{1, \ldots, k_i\}$. Set

$$f := \big(\diamond_{i=1}^{r} f_i\big) = \big(\diamond_{i=1}^{r} \diamond_{j=1}^{k_i} f_{i,j}\big).$$

Since $\omega\big(\deg(f_1) \cdots \deg(f_r)\big) < r$ by assumption, it follows that

$$k := \sum_{i=1}^{r} k_i \geq r > \omega\left(\prod_{i=1}^{r} \deg f_i\right) = \omega\left(\prod_{i=1}^{r} \prod_{j=1}^{k_i} \deg f_{i,j}\right) = \omega(\deg f)\,.$$

Then $\omega(\deg f)$ is strictly less than the number k of non-linear nearly indecomposable polynomials in its decomposition. For any prime p not dividing $f(0)$ and C_f, the assumption f irreducible modulo p would yield $k \leq \omega(\deg f)$ by Theorem 5.1: a contradiction. □

EXAMPLE. The following polynomials are irreducible over $\mathbb{Z}$ but reducible over $\mathbb{F}_p$ for all primes p:

(1) $x^{12}-x^{10}+3x^8+4x^6+3x^4+2x^2+1 = (x^2+1)\diamond(x^2+x+1)\diamond(x^3+x^2+1)$,
(2) $x^8+2x^4+x^2+1 = (x^2+1)\diamond(x^4+x+1)$,
(3) $x^4+(a^2-2)x^2+1 = (x^2+1)\diamond(x^2+ax+1)$ when $a \notin \{0,\pm 2\}$,
(4) $x^4+(a^2+2)x^2+1 = (x^2+1)\diamond(x^2+ax-1)$ when $a \neq 0$.

The examples given above can all routinely be verified as irreducible over $\mathbb{Z}$ by brute force or by use of a computer algebra system. Note that the polynomial $f \diamond g$ will not always be irreducible over $\mathbb{Z}$. For example, the polynomials

$$f = x^2+1 \quad \text{and} \quad g = x^2+x-2$$

verify the conditions of Corollary 5.2, but the polynomial

$$f \diamond g = (x^2+1)\diamond(x^2+x-2) = x^4+5x^2+4 = (x^2+4)(x^2+1)$$

is reducible over $\mathbb{Z}$.

EXAMPLE. Examples obtained from Theorem 5.1 can be used to produce some weaker statements about the reducibility of polynomials over finite fields. For example, it is well-known that the polynomial x^4+1 is irreducible over $\mathbb{Z}$ but reducible over every $\mathbb{F}_p$. We show a weaker statement holds for the more general polynomials $x^4+(a^2\pm 2)x^2+1$ with $a \neq 0$, by using the ring homomorphism

$$f : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X].$$

The polynomials

$$x^4+(a^2-2)x^2+1 \quad \text{with} \quad a \neq 0$$

are irreducible over $\mathbb{Z}$ but reducible over $\mathbb{F}_p$ for $p = 2$ and $p \equiv \pm 1 \pmod 8$ and the polynomials

$$x^4+(a^2+2)x^2+1 \quad \text{with} \quad a \neq 0$$

are irreducible over $\mathbb{Z}$ but reducible over $\mathbb{F}_p$ for $p = 2$ and $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$. It follows that the polynomials

$$x^4+(a^2-2)x^2+1 \quad \text{with} \quad a \neq 0$$

are reducible at least over $\mathbb{F}_{p^2}$ for every $p \equiv \pm 1 \pmod 8$ and the polynomials

$$x^4+(a^2+2)x^2+1 \quad \text{with} \quad a \neq 0$$

are reducible at least over $\mathbb{F}_{p^2}$ for $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$.

REFERENCES

[1] AYAD, M.: *On irreducible polynomials over $\mathbb{Q}$ which are reducible over $\mathbb{F}_p$ for all p*, Rocky Mountain J. Math. **40** (2010), no. 5, 1377–1389.
[2] BENFERHAT, L.—BENOUMHANI, S. M.—BOUMAHDI, R.— LARONE, J.: *Additive decompositions of polynomials over unique factorization domains*, J. Algebra Appl, **19** (2020), no. 8, 1–11.
[3] BRAWLEY, J. V.—CARLITZ, L.: *Irreducibles and the composed product for polynomials over a finite field*, Discrete Math. **65** (1987), no. 2, 115–139.

Received November 08, 2022

Leila Benferhat
National Higher School
of Artificial Intelligence
ENSIA
Route de Mahelma
Sidi Abdallah
ALGERIA
E-mail: leila.benferhat@ensia.edu.dz

Omar Kihel
Jesse Larone
Department of Mathematics and Statistics
Brock University
1812 Sir Isaac Brock Way, St. Catherines
ON L2S 3A1
CANADA
E-mail: okihel@brocku.ca
jlarone@brocku.ca

Rezki Ould Mohamed
Department of Algebra and Number Theory
LA3C Laboratory
Faculty of Mathematics
University of Science and Technology-
-Houari Boumediène
BP 32 Bab Ezzouar, Algiers
16111
ALGERIA
E-mail: ouldmohamed15@gmail.com