MATEMATIČKI VESNIK
МАТЕМАТИЧКИ ВЕСНИК
78, 2 (2026), 181–188
June 2026

research paper
оригинални научни рад
DOI: 10.57016/MV-HMLV9f07

FACTORIZATION OF CYCLOTOMIC POLYNOMIAL VALUES AT MERSENNE PRIME POLYNOMIALS

Luis H. Gallardo and Olivier Rahavandrainy

Abstract. We present new results about the factorization of $\Phi_p(M) \in \mathbb{F}_2[x]$, where p is a prime number, Φ_p is the corresponding cyclotomic polynomial, and M is a Mersenne prime polynomial. In particular, these results improve our understanding of the factorization of the sum of the divisors of M^{2h} for a positive integer h. This is related to the fixed points of the sum of divisors function σ on $\mathbb{F}_2[x]$. The factorization of composed polynomials over finite fields is not well understood, and classical results on cyclotomic polynomials primarily concern the special case where M is replaced by x.

1. Introduction

A *Mersenne (prime) polynomial* over $\mathbb{F}_2$ is defined as an irreducible polynomial of the form $x^a(x+1)^b + 1$, for some positive integers a and b. Since $-1 = 1$ in $\mathbb{F}_2$, this definition mirrors the concept of a Mersenne prime over the integers, where $x^a(x+1)^b \in \mathbb{F}_2[x]$ corresponds to the power $2^{a+b} \in \mathbb{Z}$.

For a nonzero polynomial $A \in \mathbb{F}_2[x]$, let $\omega(A)$ and $\sigma(A)$ denote, respectively, the number of distinct irreducible factors of A and the sum of all its divisors. If $\sigma(A) = A$, we call A *perfect* (see [12]). The integer analogue of perfect polynomials $A \in \mathbb{F}_2[x]$ is the class of multiperfect numbers $n \in \mathbb{Z}$, where $\sigma(n)/n$ is an integer.

Conjecture 1.2, central to this study, plays a crucial role in characterizing known perfect polynomials over $\mathbb{F}_2$. This conjecture has been explored in prior works, such as [10, 11, 13].

Let Φ_p denote the cyclotomic polynomial associated with a prime p. It is evident that $\Phi_p(M) = 1 + M + \cdots + M^{p-1} = \sigma(M^{p-1})$. Thus, insights into the factorization of $\Phi_p(M)$ are potentially valuable for addressing Conjecture 1.2.

The factorization of composed polynomials $F(x) = D(x)^{\deg(f(x))} \cdot f(g(x))$, where $f(x), C(x), D(x) \in \mathbb{F}_q[x]$, $D(x) \neq 0$, and $g(x) = C(x)/D(x)$, is an active area of research (see [1, 2, 5, 6, 8, 15, 17, 18, 20–24, 26]). Gallardo [9] established preliminary

2020 Mathematics Subject Classification: 11T55, 11T06
Keywords and phrases: Cyclotomic polynomials; sum of divisors; finite fields.

results for the case where $D(x) = 1$, $f(x) = \Phi_p(x)$, and $g(x) = M$, with M a Mersenne prime polynomial.

More broadly, the factorization of polynomials over finite fields (see [16, 25]) is of significant interest due to its applications in error-correcting codes, cryptography, and combinatorics. Recent works, such as [4, 14, 19], have focused on the irreducible factors of the polynomial $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Notation

We adopt the following notation:

- $\mathcal{M}$ denotes the set of all Mersenne prime polynomials over $\mathbb{F}_2$.
- For $S \in \mathbb{F}_2[x]$, define:
  - $\overline{S}$ as the polynomial obtained by replacing x in S with $x+1$: $\overline{S}(x) = S(x+1)$,
  - $\alpha_l(S)$ as the coefficient of x^{s-l} in S, where $0 \le l \le s$, and $\alpha_0(S) = 1$.
- $\mathbb{N}$ (resp. $\mathbb{N}^*$) denotes the set of nonnegative (resp. positive) integers.
- For a Mersenne prime polynomial $M := 1 + x^a(x+1)^b$ and a prime $p := 2h+1$, we use the following notation:

$$\begin{aligned} &U_{2h} := \sigma(\sigma(M^{2h})), \quad W := W_M := U_{2h} + \sigma(M^{2h}) + 1, \\ &R := R_M := \sigma(M^{2h-1}) + W, \quad \deg_M := \deg(M) = a + b, \\ &c := c_M := 2h \deg_M - \deg(W), \quad c \equiv \deg(W) \mod 2, \\ &m := m_M, \end{aligned}$$

where m is the smallest odd integer such that $\alpha_m(W) = 1$, provided that $\deg(W)$ is even (see Lemma 2.6).

A polynomial S *splits* if 0 and 1 are its only roots in $\mathbb{F}_2$. We use $\#\Gamma$ to denote the cardinality of a set Γ.

Main results

By Corollary 2.8, for a prime $p \ge 5$, we define:

$$\begin{aligned} &\Sigma_p^1 := \{M \in \mathcal{M} : c_M = \deg_M\}, \quad \Sigma_p^2 := \{M \in \mathcal{M} : c_M = \deg_M + 1,\ c_M \text{ odd}\}, \\ &\Sigma_p^3 := \{M \in \mathcal{M} : c_M + m_M = \deg_M,\ c_M \text{ even}\}, \\ &\Sigma_p^4 := \{M \in \mathcal{M} : c_M + m_M = \deg_M + 1,\ c_M \text{ even and } m_M \ge 3\}, \\ &\Sigma_p := \Sigma_p^1 \cup \Sigma_p^2 \cup \Sigma_p^3 \cup \Sigma_p^4. \end{aligned}$$

THEOREM 1.1. *Let $p \ge 5$ be a prime number. Then, for any $M \notin \Sigma_p$, $\Phi_p(M) = \sigma(M^{p-1})$ is divisible by a non-prime Mersenne polynomial.*

This theorem provides progress toward proving Conjecture 1.2, which asserts:

CONJECTURE 1.2 ([10, Conjecture 5.2]). *Let $h \in \mathbb{N}^*$ and $M \in \mathcal{M}$ such that $M \notin \{1 + x + x^3, 1 + x^2 + x^3\}$ or $h \ge 2$. Then, $\sigma(M^{2h})$ is divisible by a non-prime Mersenne polynomial.*

REMARK 1.3. The conditions defining the sets Σ_p^j are restrictive. For various p and d, the cardinality $\#\Lambda_{p,d}^j$ (where $\Lambda_{p,d}^j := \{M \in \Sigma_p^j : 5 \leq \deg(M) \leq d\}$) is often small or zero. The following table summarizes some cases, where $\mathcal{M}_d$ denotes the set of Mersenne prime polynomials with $5 \leq \deg(M) \leq d$:

p	d	$\#\Lambda_{p,d}^1$	$\#\Lambda_{p,d}^2$	$\#\Lambda_{p,d}^3$	$\#\Lambda_{p,d}^4$	$\#\mathcal{M}_d$
5	100	4	0	0	0	226
7	100	0	0	2	2	226
11	100	2	0	2	0	226
13	100	0	2	0	0	226
17	100	2	0	0	0	226
19	100	0	0	0	0	226
23	100	0	0	0	0	226
29	100	4	0	2	0	226
53	60	4	0	4	0	138
59	60	0	0	0	0	138
61	60	4	2	0	0	138
67	60	0	0	0	0	138
71	60	0	2	0	0	138

Table 1

As shown in Table 1, the sets Σ_p^j contribute only a small fraction of the Mersenne prime polynomials in $\mathcal{M}$, particularly for large p or degrees d. This indicates the broad applicability of Theorem 1.1 to Mersenne polynomials outside Σ_p. These results not only address specific cases of Conjecture 1.2 but also suggest potential paths for proving it in greater generality.

We mainly prove Theorem 1.1 by contradiction, either to Corollary 2.5 or to Lemma 2.6 (iii).

The paper is technical in nature but fundamentally relies on a simple argument: two polynomials $A(x), B(x) \in \mathbb{F}_2[x]$ are equal if and only if all their coefficients are identical.

Beard et al. [3] have previously employed a variant of this argument for the case $B(x) = \sigma(A(x))$. Canaday [7] introduced and demonstrated that certain combinations of coefficients remain invariant or undergo predictable changes when $A(x)$ is transformed into $B(x) = \sigma(A(x))$. In this paper, we further investigate these coefficient properties in Section 2, aiming to derive more general results pertinent to our problem.

2. Useful facts

In Section 3, we will use Lemmas 2.1, 2.2, 2.9, and Corollary 2.12 – sometimes without explicit mention.

LEMMA 2.1. *Let $S, T \in \mathbb{F}_2[x]$ be such that $s = \deg(S) > t = \deg(T)$. Then*
(i) $\alpha_l(S+T) = \alpha_l(S)$ for any $0 \le l < s-t$ and $\alpha_l(S+T) = \alpha_l(S) + \alpha_{l-(s-t)}(T)$ for any $s-t \le l \le s$.

(ii) $\alpha_l(\sigma(S)) = \alpha_l(S)$ for any $0 \le l \le r$, if no irreducible polynomial of degree at most r divides S.

Proof. (i) follows from the definition of α_l and (ii) from (i), since $\sigma(S) = S+T$ where $t = \deg(T) \le \deg(S) - r - 1 < s - r$. □

LEMMA 2.2. *Let $M = x^a(x+1)^b + 1 \in \mathcal{M}$ and $h \ge 1$. Then*
(i) $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h})$ if $1 \le l \le a+b-1$,

(ii) $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h} + M^{2h-1})$ if $a+b \le l \le 2(a+b)-1$.

Proof. Since $\sigma(M^{2h}) = M^{2h} + M^{2h-1} + T$, with $\deg(T) \le (a+b)(2h-2) = 2h(a+b) - 2(a+b)$, Lemma 2.1 (ii) implies that $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h})$ if $1 \le l \le a+b-1$, and $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h} + M^{2h-1})$ if $a+b \le l \le 2(a+b)-1$. □

LEMMA 2.3. *[11, Lemma 4.6] Let $M = x^a(x+1)^b + 1 \in \mathcal{M}$ and $h \ge 1$. Then, $\sigma(M^{2h})$ is square-free and it is not a Mersenne prime polynomial.*

For the remainder of the paper, we fix $M = x^a(x+1)^b + 1 \in \mathcal{M}$ and a prime $p = 2h+1$. We will frequently refer to the notation introduced in Section 1, including the polynomials W, R, U_{2h}, and the integers c and m.

Assuming that $\sigma(M^{2h})$ is divisible only by Mersenne prime polynomials, we will derive several contradictions. By Lemma 2.3, we can write:

$$\sigma(M^{2h}) = \prod_{j \in J} M_j, \quad M_j = 1 + x^{a_j}(x+1)^{b_j}, \tag{1}$$

where M_j is irreducible and $M_i \ne M_j$ if $i \ne j$.

LEMMA 2.4. *[11, Lemma 4.8] One has $M \ne 1 + x + x^2$, i.e., $a \ge 2$ or $b \ge 2$.*

COROLLARY 2.5. *(i) The integers $u = \sum_{j \in J} a_j$ and $v = \sum_{j \in J} b_j$ are both even.*

(ii) The polynomial U_{2h} splits. It is a square so that $\alpha_k(U_{2h}) = 0$ for any odd positive integer k.

Proof. (i) See [11, Corollary 4.9].

(ii) Assumption (1) implies that

$$U_{2h} = \sigma(\sigma(M^{2h})) = \sigma\Big(\prod_{j \in J} M_j\Big) = \prod_{j \in J} x^{a_j}(x+1)^{b_j} = x^u(x+1)^v,$$

where u and v are even. □

LEMMA 2.6. *The polynomials M, W and R satisfy:*
(i) $\deg_M \geq 5$ *and* $\omega(\sigma(M^{2h})) \geq 3$.

(ii) $W \neq 0$ *and it is not a square.*

(iii) R *is a square so that* $\alpha_k(R) = 0$ *for any odd positive integer* k.

(iv) $M^{2h-1} + W$ *is not a square.*

(v) There exists a least odd integer $m \geq 1$ *such that* $\alpha_m(W) = 1$ *if* $\deg(W)$ *is even.*

(vi) There exists a least even integer $e \geq 2$ *such that* $\alpha_e(W) = 1$ *if* $\deg(W)$ *is odd.*

Proof. (i) The cases where $\deg(M) \leq 4$ or $\omega(\sigma(M^{2h})) \leq 2$ are already addressed in [13].

(ii) If $0 = W = U_{2h} + \sigma(M^{2h}) + 1$, then $\sigma(M^{2h}) = U_{2h} + 1$ is a square by Corollary 2.5 (ii). This contradicts Lemma 2.3. If W is a square, then $\sigma(M^{2h}) = U_{2h} + 1 + W$ is also a square, which is impossible.

(iii) We have $R = \sigma(M^{2h-1}) + W = U_{2h} + 1 + M^{2h}$ which is a square.

(iv) If $M^{2h-1} + W = R + \sigma(M^{2h-2})$ is a square, then $\sigma(M^{2h-2})$ is a square, with $2h - 2 \geq 2$. It is impossible.

(v) This part follows from the fact that W is not a square.

(vi) If for any even e, $\alpha_e(W) = 0$, then $W + x^{\deg(W)}$ is a square. So, by differentiating relative to x, we obtain $0 = (W + x^{\deg(W)})' = W' + x^{\deg(W)-1}$. We get then the following contradiction: $x^{\deg(W)-1} = W' = (R + \sigma(M^{2h-1}))' = 0 + (\sigma(M^{2h-1}))' = (\sigma(M^{2h-1}))'$. □

COROLLARY 2.7. *If* $c \neq a + b$, *then* $\min(c, a + b)$ *is even.*

Proof. If $c < a + b$, then $\deg(W) > \deg(\sigma(M^{2h-1}))$ and $2h(a + b) - c = \deg(W) = \deg(R)$ which is even.

If $c > a+b$, then $\deg(W) < \deg(\sigma(M^{2h-1}))$ and $(2h-1)(a+b) = \deg(\sigma(M^{2h-1})) = \deg(R)$ which is even. □

COROLLARY 2.8. *If* $c = a + b + 1$ *(resp.* $c + m = a + b$ *or* $c + m = a + b + 1$ *with* $m \geq 3$*), then* c *is odd (resp. even).*

Proof. If $c = a + b + 1$, then $c > a + b$. So, $a + b = \min(c, a + b)$ is even.

If $c+m = a+b$ or $c+m = a+b+1$ with $m \geq 3$, then $c < a+b$. So, $c = \min(c, a+b)$ is even. □

LEMMA 2.9. *One has the following:*
(i) For any odd integer $l \geq 1$, $\alpha_l(M^{2h}) = 0$.

(ii) If b *is odd, then* $\alpha_1(M^{2h-1}) = 1$.

Proof. (i) This result holds because M^{2h} is a square.

(ii) $\alpha_1(M^{2h-1}) = \alpha_1(x^{(2h-1)b} \cdot (x + 1)^{(2h-1)b}) = \alpha_1((x + 1)^{(2h-1)b}) = 1$, since $(2h - 1)b$ is odd. □

Through direct computations, we obtain the following two lemmas.

LEMMA 2.10. *Let $S, T \in \mathbb{F}_2[x]$ such that $\deg(S) = \deg(T)$.*

If $\deg(S)$ is even (resp. odd), then $S+T$ is a square if and only if for any odd (resp. even) positive integer ℓ, one has $\alpha_\ell(S) = \alpha_\ell(T)$.

LEMMA 2.11. *Let $S, T \in \mathbb{F}_2[x]$ such that $\deg(S) = \deg(T)$. Then $\deg(S+T) = \deg(S) - \ell$ where ℓ is the least integer such that $\alpha_\ell(S) \neq \alpha_\ell(T)$.*

COROLLARY 2.12. *(i) If $a+b$ is odd, then $\alpha_{a+b}(M^{2h} + M^{2h-1}) = 1$.*

(ii) If $a+b$ is even, then $\alpha_1(\sigma(M^{2h-1})) = 1 = \alpha_{a+b+1}(M^{2h} + M^{2h-1})$.

Proof. We apply Lemma 2.1 with $S = M^{2h}$, $T = M^{2h-1}$. We get $s = 2h(a+b)$ and $t = (2h-1)(a+b)$ so that $s - t = a + b$. Observe that for any odd integer l, $\alpha_l(S) = 0$, since S is a square.

(i) If $a+b$ is odd, then $\alpha_{a+b}(S+T) = \alpha_{a+b}(S) + \alpha_0(T) = 0 + 1 = 1$.

(ii) If $a+b$ is even, then a and b are both odd. So, $\alpha_1(\sigma(M^{2h-1})) = \alpha_1(M^{2h-1}) = 1$ by Lemma 2.9 (ii). Thus, $\alpha_{a+b+1}(M^{2h} + M^{2h-1}) = \alpha_{a+b+1}(S) + \alpha_1(T) = 0 + \alpha_1(M^{2h-1}) = 1$. □

COROLLARY 2.13. *The integer c is the least one such that $\alpha_c(U_{2h}) + \alpha_c(\sigma(M^{2h})) = 1$.*

Proof. Remark that $\deg(S+T) = \deg(W) = 2h\deg(M) - c = \deg(S) - c$ and apply Lemma 2.11 with $S = U_{2h}$ and $T = \sigma(M^{2h}) + 1$. □

3. The proof

We consider four cases under the assumption that $M \notin \Sigma_p$. However, Corollary 2.8 eliminates **Case IV**.

Case I $c \geq a + b + 2$;

Case II $c + m < a + b$;

Case III $c < a + b < c + m$;

Case IV ($c = a+b+1$, with c even) or ($c+m = a+b$, with c odd) or ($c+m = a+b+1$, with c odd and $m \geq 3$).

For the remaining three cases, we establish four lemmas that contradict Corollary 2.5 (ii) or Lemma 2.6 (iii).

Case I $c \geq a + b + 2$

LEMMA 3.1. *If $a+b$ is odd (resp. even), then $\alpha_{a+b}(U_{2h}) = 1$ (resp. $\alpha_{a+b+1}(U_{2h}) = 1$).*

Proof. Write: $U_{2h} = (\sigma(M^{2h})) + (W+1) = S + T$, with $\deg(S) - \deg(T) = c$.

One has $a+b, a+b+1 < c$ and $a+b, a+b+1 < 2(a+b) - 1$.

By Lemma 2.1 and Corollary 2.12, we get:

$$\alpha_{a+b}(U_{2h}) = \alpha_{a+b}(\sigma(M^{2h})) = \alpha_{a+b}(M^{2h} + M^{2h-1}) = 1 \quad \text{if } a+b \text{ is odd,}$$

$$\alpha_{a+b+1}(U_{2h}) = \alpha_{a+b+1}(\sigma(M^{2h})) = \alpha_{a+b+1}(M^{2h} + M^{2h-1}) = 1 \quad \text{if } a+b \text{ is even.}$$

□

Case II $c + m < a + b$

LEMMA 3.2. *The integer $c + m$ is odd and $\alpha_{c+m}(U_{2h}) = 1$.*

Proof. Since $c < a + b$, Corollary 2.7 implies that both c and $\deg(W)$ are even.

We consider the odd integer m (of Lemma 2.6 (iv)) such that $\alpha_m(W) = 1$. Hence, $c + m = 2h \deg_M - \deg(W) + m$ is odd.

We recall that $W = 1 + \sigma(M^{2h}) + U_{2h} = 1 + \sigma(M^{2h}) + x^u(x + 1)^v$ and $R = \sigma(M^{2h-1})+W$ is a square. Write $U_{2h} = S+T$ with $S = M^{2h}$ and $T = W+\sigma(M^{2h-1})+1$. One has that $\deg(S) - \deg(T) = 2h(a + b) - \deg(W) = c$. Lemma 2.1 implies that $\alpha_{c+m}(U_{2h}) = \alpha_{c+m}(M^{2h}) + \alpha_m(T) = 0 + \alpha_m(T) = \alpha_m(T)$. But, $m < a + b - c = \deg(W)-\deg(\sigma(M^{2h-1})+1)$. Again, from Lemma 2.1, one has $\alpha_m(T) = \alpha_m(W) = 1$. So, $\alpha_{c+m}(U_{2h}) = 1$. □

Case III $c < a + b < c + m$

As above, c and $\deg(W)$ are both even.

LEMMA 3.3. *If $c + m > a + b$ and $a + b$ odd, then $\alpha_{a+b-c}(R) = 1$.*

Proof. Set $R = S + T$ with $S = W$ and $T = \sigma(M^{2h-1})$. One has $\deg(S) - \deg(T) = a+b-c$ and $a+b-c < m$. Therefore, $\alpha_{a+b-c}(W) = 0$ and $\alpha_{a+b-c}(R) = \alpha_{a+b-c}(W)+\alpha_0(\sigma(M^{2h-1})) = 0 + 1 = 1$. □

LEMMA 3.4. *If $c + m > a + b + 1$ and $a + b$ even, then $\alpha_{a+b-c+1}(R) = 1$.*

Proof. Again, set $S = W$ and $T = \sigma(M^{2h-1})$. One has $\deg(S) - \deg(T) = a + b - c$ and $a + b - c + 1 < m$. By Corollary 2.12, we obtain $\alpha_1(\sigma(M^{2h-1})) = 1$. So, $\alpha_{a+b-c+1}(R) = \alpha_{a+b-c+1}(W) + \alpha_1(\sigma(M^{2h-1})) = 0 + 1 = 1$. □

3.1 Final remark

We have shown that if $M \notin \Sigma_p$, this leads to a contradiction regarding the squareness of W and R: $\alpha_\ell(W) = 1$ or $\alpha_\ell(R) = 1$, where ℓ is odd and $\ell \leq \deg(M)$.

When $M \in \Sigma_p$, computational evidence reveals the same contradiction, but for $\ell > \deg(M)$. For this case, alternative methods are required.

REFERENCES

[1] S. Agou, *Irréducibilité des polynômes $f(x^{p^r} - ax)$ sur un corps fini $\mathbb{F}_{p^s}$*, J. Reine Angew. Math., **292** (1977), 191–195.

[2] O. Ahmadi, M.-S. Khosro, *A note on the stability of trinomials over finite fields*, Finite Fields Appl., **63** (2020), 101649, 13 pp.

[3] J. T. B. Beard Jr., J. R. O'Connell Jr., K. I. West, *Perfect polynomials over $GF(q)$*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat., **62(8)** (1977), 283–291.

[4] F.-E. Brochero-Martínez, C. R. Giraldo, L. B. de Oliveira, *Explicit factorization of $x^n - 1 \in \mathbb{F}_q[x]$*, Des. Codes Cryptogr., **77(1)** (2015), 277–286.

[5] F.-E. Brochero-Martínez, L. Reis, *Factoring polynomials of the form $f(x^n) \in \mathbb{F}_q[x]$*, Finite Fields Appl., **49** (2018), 166–179.

[6] M. C. R. Butler, *The irreducible factors of $f(x^m)$ over a finite field*, J. London Math. Soc., **30** (1955), 480–482.

[7] E. F. Canaday, *The sum of the divisors of a polynomial*, Duke Math. J., **8** (1941), 721–737.

[8] S. D. Cohen, *The irreducibility of compositions of linear polynomials over a finite field*, Compositio Math., **47** (1982), 149–152.

[9] L. H. Gallardo, *On the prime factors of* $\Phi_p(M)$, Integers, **21** (2021), Paper No. A70, 12 pp.

[10] L. H. Gallardo, O. Rahavandrainy, *On even (unitary) perfect polynomials over* $\mathbb{F}_2$, Finite Fields Appl., **18(5)** (2012), 920–932.

[11] L. H. Gallardo, O. Rahavandrainy, *On Mersenne polynomials over* $\mathbb{F}_2$, Finite Fields Appl., **59** (2019), 284–296.

[12] L. H. Gallardo, O. Rahavandrainy, *A polynomial variant of perfect numbers*, J. Integer Seq., **8** (2020), Art. 20.8.6, 9pp.

[13] L. H. Gallardo, O. Rahavandrainy, *All even (unitary) perfect polynomials over* $\mathbb{F}_2$ *with only Mersenne primes as odd divisors*, Kragujevac J. Math., **49(4)** (2025), 639–652.

[14] D. R. Heath-Brown, G. Micheli, *Irreducible polynomials over finite fields produced by composition of quadratics*, Rev. Mat. Iberoam., **35(3)** (2011), 847–855.

[15] M. K. Kyuregyan, G. H. Kyuregyan, *Irreducible compositions of polynomials over finite fields*, Des. Codes Cryptogr., **61(3)** (2011), 301–314.

[16] R. Lidl, H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications,* 20, Cambridge: Cambridge University Press. xiv, 1996.

[17] A. F. Long, *Factorization of irreducible polynomials over a finite field with the substitution* $x^{q^r} - x$ *for* x, Acta Arith., **25** (1973), 65–80.

[18] A. F. Long, T. P. Vaughan, *Factorization of* $Q(h(T))(x)$ *over a finite field where* $Q(x)$ *is irreducible and* $h(T)(x)$ *is linear I*, *Linear Albegra Appl.*, **13** (1976), 207–221.

[19] D. Oliveira, L. Reis, *On polynomials* $x^n - 1$ *over binary fields whose irreducible factors are binomials and trinomials*, Finite Fields Appl., **73** (2021), Paper NO. 101837, 11 pp.

[20] D. Panario, L. Reis, Q. Wang, *Construction of irreducible polynomials through rational transformations*, J. Pure Appl. Algebra, **224(5)** (2020), 106241, 17 p.

[21] E. L. Petersson, *Über die Irreduzibilität ganzahliger Polynome nach einem Primzahlmodul*, J. Reine Angew. Math., **175** (1936), 209–220.

[22] L. Reis, *Factorization of a class of composed polynomials*, Des. Codes Cryptogr., **87(7)** (2019), 1657–1671.

[23] L. Reis, *On the factorization of iterated polynomials*, Rev. Mat. Iberoam., **36(7)** (2020), 1957–1978.

[24] I. Seres, *Lősung und Verallgemeinerung eines Schursten Irreduzibilitătsproblems fűr Polynome*, Acta Math. Acad. Sci. Hungar., **7** (1956), 151–157.

[25] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math., **12** (1962), 1099–1106.

[26] M. Ulas, *Is every irreducible polynomial reducible after a polynomial substitution ?*, J. Number Theory, **202** (2019), 37–59.

(received 17.05.2024; in revised form 16.12.2024; available online 01.07.2025)

University Brest, UMR CNRS 6205, Laboratoire de Mathématiques de Bretagne Atlantique, France
E-mail: luis.gallardo@univ-brest.fr
ORCID iD: https://orcid.org/0000-0002-4564-5393

University Brest, UMR CNRS 6205, Laboratoire de Mathématiques de Bretagne Atlantique, France
E-mail: olivier.rahavandrainy@univ-brest.fr
ORCID iD: https://orcid.org/0009-0008-6232-1156