MATHEMATICA, 66 (89), N° 1, 2024, pp. 44–62

STABILITY OF BINOMIALS OVER FINITE FIELDS

MOHAMED AYAD, BOUALEM BENSEBA, and MOHAMED MADI

Abstract. A polynomial $f(x)$ over a field K is said to be stable if all its iterates are irreducible over K. L. Danielson and B. Fein have shown that over a large class of fields K, if $f(x)$ is an irreducible monic binomial, then it is stable over K. In this paper it is proved that this result no longer holds over finite fields. Necessary and sufficient conditions are provided under which a given binomial is stable over $\mathbb{F}_q$. These conditions are used to construct a table listing the stable binomials over $\mathbb{F}_q$ of the form $f(x) = x^d - a$, $a \in \mathbb{F}_q \setminus \{0, 1\}$, for $q \leq 27$ and $d \leq 10$. The paper ends with a brief link to Mersenne primes.

MSC 2020. 11T06, 11T55, 12E05.

Key words. Irreducibility, iteration, stability, finite fields, Mersenne primes.

1. INTRODUCTION

Let K be a field and $f(x)$ be a non-constant polynomial with coefficients in K. Set $f_0(x) = x$, $f_1(x) = x$ and $f_n(x) = \Big(f_{n-1} \circ f\Big)(x)$ for $n \geq 2$. Following R. W. K. Odoni [8], this polynomial is said to be stable over K if $f_n(x)$ is irreducible over K for all $n \geq 0$. The first example of such a polynomial appears in [8], where it is proved that $f(x) = x^2 - x + 1$ is stable over $\mathbb{Q}$. In [9], the same author shows that any iterate of an Eiseistein polynomial is itself Eisenstein, thus $f(x)$ is stable. This gives a class of stable polynomials over fraction fields of factorial domains.

This result implies that, given an integral domain A with fraction field K and algebraically independent variables $s_1, s_2, \ldots, s_n$, the generic polynomial of degree n,

$$G(s_1, \ldots, s_n, x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n \in A[s_1, \ldots, s_n][x]$$

is stable over $K(s_1, \ldots, s_n)$.

Inspired by this result, the paper [2] considers the stability of the generic polynomial of the integers of a number field. More precisely, let K be a number field of degree n and $\{\omega_1, \ldots, \omega_n\}$ be an integral basis. Let $u_1, \ldots, u_n$

Corresponding author: Mohamed Ayad.

DOI: 10.24193/mathcluj.2024.1.04

be independent variables over $\mathbb{Q}$ and let

$$(u_1, \ldots, u_n, x) = \prod_{i=1}^{n} \Big(x - (u_1\omega_1^{\sigma_i} + \cdots + u_n\omega_n^{\sigma_i} \Big),$$

where $\sigma_1, \ldots, \sigma_n$ are the distinct embeddings of K in $\mathbb{C}$. Then under some arithmetical conditions, this polynomial is stable over $\mathbb{Q}(u_1, \ldots, u_n)$. To the best of our knowledge, the stability of the polynomial F in the general case is still open.

The stability of quadratic polynomials over various fields was the subject of [3] and [4].

For the stability of trinomials over finite fields, we refer to [1].

In [5], the following surprising result is proved. Let $f(x) = x^n - b$ be an irreducible polynomial over K. Then $f(x)$ is stable over K in the following cases:

(i) $K = \mathbb{Q}$ and $b \in \mathbb{Z}$.
(ii) $K = \mathbb{Q}(t)$ and $b \in \mathbb{Z}[t]$.
(iii) $K = F(t)$ and $b \in F[t]$, where F is an arbitrary algebraically closed field.
(iv) $K = F(t)$, $b \in F(t) \setminus F$, $n \geq 3$ and F is an arbitrary field of characteristic 0.

We will see in the last section of this paper that this result does not hold over finite fields. We will give an algorithm which establishes the stability of a given binomial defined over a finite field.

For fixed integer $d \geq 2$, define inductively the polynomials $(P_n(x))_{n\geq 1}$ by $P_1(x) = x$ and $P_n(x) = [P_{n-1}(x)]^d + (-1)^{d-1}x$ for $n \geq 2$.

Let $a \in \mathbb{F}_q^\star$ and let n_0 and m_0 be indices with $n_0 < m_0$ such that $P_{n_0}(a) = P_{m_0}(a)$. Supposing that n_0 first and m_0 next are chosen to be minimal with this property, then $\{P_n(a), n \geq 1\} = \{P_1(a), \ldots, P_{m_0-1}(a)\}$. This set plays an important role in the stability of $f(x) = x^d - a$. In section 4, the following result is proved.

THEOREM 1.1. *Let $d \geq 2$ be an integer such that $d \neq 0 \pmod 4$ and let $f(x) = x^d - a \in \mathbb{F}_q[x]$. Let n_0, m_0, with $n_0 < m_0$, be minimal integers such that $P_{n_0}(a) = P_{m_0}(a)$. Then $f(x)$ is stable over $\mathbb{F}_q$ if and only if for any prime number $l \mid d$ and any $k \in \{1, ..., m_0 - 1\}$, $P_k(a) \notin \mathbb{F}_q^l$. Here $P_k(a) \notin \mathbb{F}_q^l$ means in particular $P_k(a) \neq 0$.*

This theorem is used for the construction of the table placed at the end of the paper. Obviously, the integer m_0 defined above satisfies the condition $m_0 \leq q+1$. Theorem 4.4 shows that $m_0 \leq (q-1)/\delta+2$, where $\delta = gcd(q-1, d)$. There are examples where this bound is reached. Suppose that $f(x)$ is not stable and let $r_0 \geq 1$ be the smallest integer such that $f_{r_0-1}(x)$ is irreducible and $f_{r_0}(x)$ is reducible over $\mathbb{F}_q$. The preceding theorem implies $r_0 \leq m_0 - 1 \leq (q-1)/\delta + 1$. Notice that this bound for r_0 depends on q.

QUESTION 1.2. *Does there exist an integer N such that for any prime power q and any $f(x) = x^d - a \in \mathbb{F}_q[x]$, if $f_1(x), \ldots, f_N(x)$ are irreducible over $\mathbb{F}_q$; then $f(x)$ is stable?*

The example $f(x) = x^2 - 12 \in \mathbb{F}_{19}[x]$ extracted from the table in section 4, shows that $f_1(x), \ldots, f_5(x)$ are irreducible while $f_6(x)$ is reducible. This shows that if N exists, then $N \geq 6$.

NOTATION 1.3. *The following notations will be used throughout the paper.*
$\mathbb{F}_q$*: the finite field with q elements.*
$lc(f)$*: leading coefficient of $f(x)$.*
$f_n(x)$*: n-th iterate of $f(x)$.*
$N_{F/K}(\alpha)$*: norm of α relatve to the extension F/K.*
$m \mid n$*: m divides n.*

2. PRELIMINARY RESULTS

LEMMA 2.1. *Let q be a power of a prime $p \neq 2$, l a prime number and δ a positive integer such that $l \mid q-1$ and $\delta \equiv 1 \pmod{l}$. Let $\alpha \in \mathbb{F}_q^*$. Then α is an l-th power in $\mathbb{F}_q^*$ if and only if α is an l-th power in $\mathbb{F}_{q^\delta}^*$.*

Proof. Let ξ be a generator of $\mathbb{F}_{q^\delta}^*$; then $\eta = \xi^{(q^\delta-1)/(q-1)}$ is a generator of $\mathbb{F}_q^*$. Set $\alpha = \eta^u$ where u is a nonnegative integer; then

$$\alpha = \xi^{u(q^\delta-1)/(q-1)} = \xi^{u(1+q+\cdots+q^{\delta-1})} := \xi^v.$$

We have $v = u(1+q+\cdots+q^{\delta-1}) \equiv u\delta \pmod{l} \equiv u \pmod{l}$, hence α is an l-th power in $\mathbb{F}_q^*$ if and only if α is an l-th power in $\mathbb{F}_{q^\delta}^*$. □

LEMMA 2.2. *Let p be an odd prime number and $q = p^m$ with $m \geq 1$. Let $k \geq 1$ be an integer and $\alpha \in \mathbb{F}_{q^k}^*$. The following equivalences hold.*

(i)

$$\alpha \textit{ is a square in } \mathbb{F}_{q^k} \iff \alpha^{(q^k-1)/2} = 1.$$

(ii)

$$-1 \textit{ is a square in } \mathbb{F}_{q^k} \iff \begin{cases} k & \textit{is even or,} \\ k & \textit{is odd and } q \equiv 1 \pmod{4}. \end{cases}$$

Proof. Let ξ be a generator of $\mathbb{F}_{q^k}^*$ and set $\alpha = \xi^u$, $u \geq 0$. Then
(i)

$$\begin{aligned} \alpha^{(q^k-1)/2} = 1 &\iff \xi^{u(q^k-1)/2} = 1 \\ &\iff u(q^k-1)/2 \equiv 0 \pmod{q^k-1} \\ &\iff u \equiv 0 \pmod{2} \\ &\iff \alpha \text{ is a square in } \mathbb{F}_{q^k}. \end{aligned}$$

(ii) By (i) we have:

$$\begin{aligned}
-1 \text{ is a square in } \mathbb{F}_{q^k} &\iff (-1)^{(q^k-1)/2} = 1 \\
&\iff (q^k-1)/2 \equiv 0 \pmod 2 \\
&\iff q^k - 1 \equiv 0 \pmod 4 \\
&\iff q^k \equiv 1 \pmod 4 \\
&\iff k \text{ is even or } k \text{ is odd and } q \equiv 1 \pmod 4.
\end{aligned}$$

□

LEMMA 2.3. *Let $\delta \geq 1$ an integer, $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^\delta}$.*

1. *The norm map $N_{F/K} : F \to K$ is surjective and it maps F^* onto K^*.*

2. *Let ξ be a generator of F^* and $\eta = \xi^{(q^\delta-1)/(q-1)}$. Then η is a generator of K^*.*

3. *Let l be a prime number. If $l \nmid q-1$, then the morphism $\Phi_l : F^* \to K^*$ such that $\Phi_l = x^l$ is one-to-one and onto. If $l \mid q-1$, then $Ker(\Phi_l) = \{x \in F^* \mid x^l = 1\}$ and $(F^*/Ker(\Phi_l)) \simeq (K^*)^l$. Moreover, for any $a \in F^*$, $a \in (F^*)^l$ if and only if $N_{F/K}(a) \in (K^*)^l$.*

Proof. 1. See [7, Theorem 2.28].

2. Since F^* is cyclic of order $q^\delta - 1$ generated by ξ, it contains a unique subgroup of order $q-1$ generated by $\eta = \xi^{(q^\delta-1)/(q-1)}$, namely K^*. Moreover,

$$\begin{aligned}
\eta^k &= \xi^{k(q^\delta-1)/(q-1)} = (\xi^k)^{(q^\delta-1)/(q-1)} = (\xi^k)^{1+q+\cdots+q^{\delta-1}} \\
&= (\xi^k)(\xi^k)^q \cdots (\xi^k)^{q^{\delta-1}} = N_{F/K}(\xi^k).
\end{aligned}$$

3. The statements about Φ_l are obvious. We prove the last statement of 3. Set $a = \xi^k$ for some $k \geq 0$. Then

$$N_{F/K}(a) = [N_{F/K}(\xi)]^k = [\xi^{(q^\delta-1)/(q-1)}]^k = \eta^k,$$

hence

$$a \in (F^*)^l \Leftrightarrow k \equiv 0 \pmod l \Leftrightarrow N_{F/K}(a) \in (K^*)^l.$$

□

We will make use of the following Lemma the proof of which is immediate.

LEMMA 2.4. *Let K be a field, $\lambda \in K^\star$ and $u(x) = \lambda x$. Let $f(x) \in K[x] \setminus K$ and $g(x) = \big(u^{-1} \circ f \circ u\big)(x)$. Then, for any $n \geq 1$, $f_n(x)$ and $g_n(x)$ have the same number of irreducible factors over K.*

3. IRREDUCIBILITY OF BINOMIALS

In this section, we study the irreducibility of binomials $f(x) = x^d - a$ with $a \in \mathbb{F}_q^\star$.

Example 3.1. Let q be a power of a prime p and $f(x) = x^d - a$, where $a \in \mathbb{F}_q^\star$. Suppose that $p \mid d$; then $f(x)$ is reducible over $\mathbb{F}_q$.

Proof. Set $d = pm$ and $q = p^k$, where m and k are positive integers. Then $f(x) = x^{pm} - a^q = (x^m)^p - (a^{p^{k-1}})^p = \left(x^m - a^{p^{k-1}}\right)\left((x^m)^{p-1} + \cdots + (a^{p^{k-1}})^{p-1}\right)$, hence $f(x)$ is reducible over $\mathbb{F}_q$. □

The proof of the following lemma can be found in [10].

Lemma 3.2. *Let K be a field and $f(x), g(x) \in K[x] \backslash K$. Let α be a root of $f(x)$ in an algebraic closure of K. Then $f \circ g(x)$ is irreducible over K if and only if $f(x)$ is irreducible over K and $g(x) - \alpha$ is irreducible over $K(\alpha)$.*

Lemma 3.3. *Let K be a field and $n \geq 2$ an integer. Let $a \in K^*$. Assume that for all prime numbers $l \mid d$, we have $a \notin K^l$ and if $4 \mid d$, then $a \notin -4K^4$. Then $x^d - a$ is irreducible over K. The converse is true.*

Proof. For the direct implication, we refer the reader to [6][Chapter 8, Theorem 16]. We prove here the converse. Let l be a prime divisor of d and $a = b^l$, with $b \in K^*$. Set $d = tl$. Then

$$\begin{aligned} x^d - a &= x^{tl} - b^l \\ &= (x^t)^l - b^l \\ &= (x^t - b)u(x^t) \text{ for some } u(X) \in K[X]. \end{aligned}$$

Thus $x^d - a$ is reducible. If $4 \mid d$, $d = 4t$ and $a = -4b^4$, then

$$x^d - a = x^{4t} + 4b^4 = (x^{2t} + 2bx^t + 2b^2)(x^{2t} - 2bx^t + 2b^2),$$

hence the result. □

This result about the irreducibility of binomials is valid over any field. In [7], the same problem of irreducibility is stated specifically over finite fields. We state Theorem 3.75 in [7].

Lemma 3.4. *Let $d \geq 2$ be an integer and $a \in \mathbb{F}_q^\star$. Then the binomial $x^d - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if the following two conditions are satisfied:*

(i) *each prime factor of d divides the order e of a in $\mathbb{F}_q^\star$ but not $(q-1)/e$;*
(ii) $q \equiv 1 \pmod 4$ *if* $d \equiv 0 \pmod 4$.

The conditions, call them (C), contained in Lemma 3.3 (resp. call them $(C^{'})$ contained in Lemma 3.4) are equivalent to the irreducibility of the binomial $x^d - a$, hence (C) and $(C^{'})$ are equivalent. But at first glance, it is not so obvious that they express the same meaning, so we prove the following.

Proposition 3.5. *Let l be a prime number and $a \in \mathbb{F}_q^\star$. Let e be the order of a in $\mathbb{F}_q^\star$. Then the following propositions are equivalent:*

(i) *$l \mid e$ and $l \nmid (q-1)/e$;*

(ii) $a \notin (\mathbb{F}_q^\star)^l$.

Proof.

- $(i) \Rightarrow (ii)$. Suppose that $a \in (\mathbb{F}_q^\star)^l$ and let ξ be a generator of $\mathbb{F}_q^\star$. Then $a = \xi^{lu}$, where u is a nonnegative integer. Moreover, we have $e = (q-1)/gcd(q-1, lu)$. Let $\delta = gcd(q-1, lu)$, then $\delta = (q-1)/e$. We show that $l \nmid e$ or $l \mid (q-1)/e$. Suppose that $l \mid e$, then $l \mid q-1$, thus $l \mid \delta$. Therefore $l \mid (q-1)/e$.
- $(ii) \Rightarrow (i)$. Suppose that $a \notin (\mathbb{F}_q^\star)^l$ and let ξ be a generator of $\mathbb{F}_q^\star$. Then $a = \xi^u$, where u is a nonnegative integer such that $u \neq 0 \pmod{l}$. Let $\delta = gcd(q-1, u)$. Since $u \neq 0 \pmod{l}$, then $l \mid q-1$; otherwise any element of $\mathbb{F}_q^\star$ is an l-th power. This implies $l \nmid \delta$ and then $l \mid (q-1)/\delta$. Since $e = (q-1)/\delta$, then $l \mid e$. Since $\delta = (q-1)/e$, then $l \nmid (q-1)/e$.

□

Corollary 3.6. *Let q be a power of a prime.*

1. *Let $d \geq 2$ be an integer such that $d \neq 0 \pmod 4$ and let $a \in \mathbb{F}_q^\star$. Suppose that $x^d - a$ is irreducible over $\mathbb{F}_q$. Then any prime factor of d divides $q-1$. Moreover, $d \mid q^d - 1$.*
2. *Let $d \geq 2$ be an integer such that $d \neq 0 \pmod 4$. Let a and $b \in \mathbb{F}_q^\star$ and let $e(a)$ and $e(b)$ be their respective orders. If $e(a) = e(b)$, then $x^d - a$ is irreducible over $\mathbb{F}_q$ if and only if the same holds for $x^d - b$.*
3. *Let $a \in \mathbb{F}_q^\star$ and let $d \neq 0 \pmod 4$. Suppose that $q \not\equiv -1 \pmod 4$, in the case d even. Then $x^d - a$ is irreducible over $\mathbb{F}_q$ if and only if the same property holds for $x^d + a$.*
4. *Let d and e be positive integers such that $d \geq 2$, $d \neq 0 \pmod 4$ and $gcd(d, e) \neq 1$. Let $a \in \mathbb{F}_q^\star$; then $x^d - a^e$ is reducible over $\mathbb{F}_q$*
5. *Let d and e be positive integers such that $d \geq 2$, $d \neq 0 \pmod 4$ and $gcd(d, e) = 1$. Let $a \in \mathbb{F}_q^\star$; then $x^d - a$ is irreducible over $\mathbb{F}_q$ if and only if $x^d - a^e$ satisfies the same property.*
6. *Let d be a positive integer such that $d \neq 0 \pmod 4$. Let $\hat{d}$ be the squarefree part of d. Let $a \in \mathbb{F}_q^\star$ and $b \in \mathbb{F}_q^{\star \hat{d}}$; then $x^d - a$ is irreducible over $\mathbb{F}_q$ if and only if $x^d - ab$ satisfies the same property.*
7. *If d_1 and d_2 have the same prime factors with d_1 and $d_2 \neq 0 \pmod 4$, then $x^{d_1} - a$ is irreducible over $\mathbb{F}_q$ if and only if $x^{d_2} - a$ is.*
8. *Let d_1, d_2 be integers at least equal to 2, $(gcd(d_1, d_2) = 1$, both not 0 modulo 4. Let $f_1(x) = x^{d_1} - a_1$, $f_2(x) = x^{d_2} - a_2$ and $f(x) = x^{d_1 d_1} - a_1^{d_2} a_2^{d_1}$, where a_1 and $a_2 \in \mathbb{F}_q^\star$. Then $f(x)$ is irreducible over $\mathbb{F}_q$ if and only if $f_1(x)$ and $f_2(x)$ have the same property.*

Proof.

1. Suppose that some prime factor l of d does not divide $q-1$; then any element $a \in \mathbb{F}_q^\star$ is an l-th power, hence $x^d - a$ is reducible over $\mathbb{F}_q$ which

is a contradiction. For the second part, let α be a root of $x^d - a$ and let $A = \{n \in \mathbb{Z}, \alpha^n \in \mathbb{F}_q\}$. Since $\alpha^{q^d-1} = 1$; then $A \neq \emptyset$. Obviously, A is an ideal of $\mathbb{Z}$. Let δ be a generator of A, then $\delta \mid d$. On the other hand, $x^d - a$ is the minimal polynomial of α over $\mathbb{F}_q$, hence $x^d - a$ divides $x^\delta - b$ for some $b \in \mathbb{F}_q^\star$. This implies $d \leq \delta$ and then $d = \delta$. Now since $q^d - 1 \in A$, then $d \mid q^d - 1$.

2. Obvious from Lemma 3.4.
3. By symmetry, we may just prove the necessity of the condition. Suppose that $x^d - a$ is reducible over $\mathbb{F}_q$ and let l be a prime number dividing d such that $a = b^l$ with $b \in \mathbb{F}_q$. If $l = 2$ and $2 \mid q-1$, then $q \equiv 1 \pmod 4$ and then, by Lemma 2.2, -1 is a square in $\mathbb{F}_q^\star$. This implies $-a$ is a square, hence $x^d + a$ is reducible. If $l = 2$ and $2 \nmid q-1$, then any element of $\mathbb{F}_q^\star$ is a square. In particular $-a$ is a square and then $x^d + a$ is reducible. If $l \neq 2$, then $-a = -b^l = (-b)^l$ and we get the same conclusion as before.
4. Let l be a prime factor of $gcd(d,e)$. Set $d = ld_1$ and $e = le_1$. Then

$$\begin{aligned} x^d - a^e &= x^{ld_1} - a^{le_1} \\ &= (x^{d_1})^l - (a^{e_1})^l = \Big(x^{d_1} - a^{e_1}\Big)\Big((x^{d_1})^{l-1} + \ldots + (a^{e_1})^{l-1}\Big), \end{aligned}$$

   hence $x^d - a$ is reducible over $\mathbb{F}_q$.
5.
   - Suppose that $x^d - a$ is reducible over $\mathbb{F}_q$ and let l be a prime number such that $l \mid d$ and $a = b^l$ with $b \in \mathbb{F}_q^\star$; then $a^e = (b^e)^l$, thus $x^d - a^e$ is reducible over $\mathbb{F}_q$.
   - Conversely, suppose that $x^d - a^e$ is reducible over $\mathbb{F}_q$ and let l be a prime number such that $l \mid d$ and $a^e = b^l$ with $b \in \mathbb{F}_q^\star$. Let u and $v \in \mathbb{Z}$ such that $ud + ve = 1$ and let δ be such that $d = l\delta$; then

     $$a = a^{ud+ve} = a^{ud}a^{ve} = \Big(a^{u\delta}\Big)^l \Big(b^v\Big)^l = \Big(a^{u\delta}b^v\Big)^l,$$

     hence $x^d - a$ is reducible over $\mathbb{F}_q$.
6.
   - Suppose that $x^d - a$ is reducible over $\mathbb{F}_q$ and let l be a prime number dividing d such that a is an l-power; then ab is also an l-th power. This implies $x^d - ab$ is reducible over $\mathbb{F}_q$.
   - Suppose that $x^d - ab$ is reducible over $\mathbb{F}_q$ and let l be a prime number dividing d such that ab is an l-th power. Multiplying by b^{-1}, which is an l-th power, shows that a is an l-th power, hence $x^d - a$ is reducible over $\mathbb{F}_q$.
7. Suppose that $x^{d_1} - a$ is reducible over $\mathbb{F}_q$ and let $l \mid d$ be a prime such that $a = b^l$ with $b \in \mathbb{F}_q^\star$. Since $l \mid d_2$, then $x^{d_2} - a$ is reducible over $\mathbb{F}_q$.
8.
   - Sufficiency of the condition. Suppose by contadiction that $f(x)$ is reducible over $\mathbb{F}_q$ and let l be a prime number dividing $d_1 d_2$

and $b \in \mathbb{F}_q^\star$ such that $a_1^{d_2} a_2^{d_1} = b^l$. We may suppose that $l \mid d_1$ and $l \nmid d_2$ since the proof is similar for the other case. Let ξ be a generator of $\mathbb{F}_q^\star$. Set $a_1 = \xi^{u_1}$, $a_2 = \xi^{u_2}$ and $b = \xi^v$; then $\xi^{u_1 d_2 + u_2 d_1} = \xi^{vl}$, hence $u_1 d_2 + u_2 d_1 \equiv vl \pmod{q-1}$. Let $w \in \mathbb{Z}$ be such that $u_1 d_2 + u_2 d_1 = vl + w(q-1)$. If $l \nmid q-1$; then $f_1(x)$ is reducible by item 1. of this corollary . Suppose next that $l \mid q-1$, then $l \mid u_1$, thus a_1 is an l-th power for a prime factor of d_1. This implies $f_1(x)$ is reducible.

- Necessity of the condition. Suppose that one of $f_1(x)$, $f_2(x)$, say $f_1(x)$, is reducible over $\mathbb{F}_q$. Let l be a prime number such that $l \mid d_1$ and $a_1 = b^l$ with $b \in \mathbb{F}_q^\star$. Let $\delta_1 \in \mathbb{Z}$ be such that $d_1 = l\delta_1$; then $a_1^{d_2} a_2^{d_1} = b^{ld_2} a_2^{l\delta_1} = \left(b^{d_2} a_2^{\delta_1}\right)^l$, hence $f(x)$ is reducible over $\mathbb{F}_q$.

$\square$

Notice that the assumptions in 1. of Corollary 3.6 hold if $gcd(d, q-1) = 1$.

4. STABILITY OF BINOMIALS

Let $d \geq 2$ be an integer. Define inductively the polynomials $(P_n(x))_{n\geq 1}$ by $P_1(x) = x$ and $P_n(x) = [P_{n-1}(x)]^d + (-1)^{d-1} x$ for $n \geq 2$. These polynomials will be used in what follows.

Lemma 4.1. *Let $d \geq 2$ be an integer such that $d \neq 0 \pmod 4$ and let $f(x) = x^d - a$, where $a \in \mathbb{F}_q{}^*$.*

1. *Suppose that $f_{n-1}(x)$ is irreducible and $f_n(x)$ is reducible over $\mathbb{F}_q$ for some $n \geq 2$. Then there exists a prime number $l \mid d$ such that $P_n(a)$ is an l-th power in $\mathbb{F}_q^\star$.*

2. *If $P_n(a) = 0$ for some $n \geq 2$, then $f(x)$ is reducible over $\mathbb{F}_q$. If for some $n \geq 1$, $P_n(a)$ is an l-th power in $\mathbb{F}_q^\star$ for some prime divisor l of d, then $f_n(x)$ is reducible over $\mathbb{F}_q$.*

Proof. 1. Let $(\alpha_n)_{n\geq 1}$ be elements of $\overline{\mathbb{F}_q}$ such that $f(\alpha_1) = 0$ and $f(\alpha_n) = \alpha_{n-1}$ for $n \geq 2$. Set $\beta_k = \alpha_k + P_{n-k}(a)$. We have $f(\alpha_n) = \alpha_n^d - a = \alpha_{n-1}$, hence α_n is a root of $x^d - a - \alpha_{n-1}$. By Lemma 3.2 this polynomial is reducible over $\mathbb{F}_q(\alpha_{n-1})$, hence by Lemma 3.3, there exists a prime number $l \mid d$ such that $a + \alpha_{n-1} = b_1^l$ for some $b_1 \in \mathbb{F}_q(\alpha_{n-1})$. Thus $P_1(a) + \alpha_{n-1} = b_1^l$, $b_1 \in \mathbb{F}_q(\alpha_{n-1})$. We prove by induction on $k \in \{1, ..., n-1\}$ that

$$P_k(a) + \alpha_{n-k} = b_k^l, \text{ with } b_k \in \mathbb{F}_q(\alpha_{n-k}). \tag{1}$$

Let $k \in \{1, ..., n-2\}$ and suppose that (1) holds. Denote by N the norm map $N_{\mathbb{F}_q(\alpha_{n-k})/\mathbb{F}_q(\alpha_{n-(k+1)})}$. Then

$$\begin{aligned} N(P_k(a) + \alpha_{n-k}) &= N(\beta_{n-k}) \\ &= [N(b_k)]^l := b_{k+1}^l, \end{aligned}$$

with $b_{k+1} \in \mathbb{F}_q(\alpha_{n-(k+1)})$. Since $\alpha_{n-k}^d - a - \alpha_{n-(k+1)} = 0$, then

$$[\beta_{n-k} - P_k(a)]^d - a - \alpha_{n-(k+1)} = 0, \tag{2}$$

hence

$$\begin{aligned} N(P_k(a) + \alpha_{n-k}) &= N(\beta_{n-k}) \\ &= (-1)^d \left\{ [-P_k(a)]^d - a - \alpha_{n-(k+1)} \right\} \\ &= [P_k(a)]^d + (-1)^{d-1} a + (-1)^{d-1} \alpha_{n-(k+1)} \\ &= P_{k+1}(a) + (-1)^{d-1} \alpha_{n-(k+1)}. \end{aligned}$$

If $d \equiv 1 \pmod 2$ we immediately obtain $P_{k+1}(a) + \alpha_{n-(k+1)} = b_{k+1}^l$ with $b_{k+1} \in \mathbb{F}_q(\alpha_{n-(k+1)})$. If $d \equiv 0(\pmod 2)$, since $\alpha_{n-(k+1)}$ and $-\alpha_{n-(k+1)}$ are conjugate over $\mathbb{F}_q(\alpha_{n-(k+2)})$ then $P_{k+1}(a) + \alpha_{n-(k+1)} = \overline{b_{k+1}}^l$ where $\overline{b_{k+1}}$ is a conjugate of b_{k+1} over $\mathbb{F}_q(\alpha_{n-(k+2)})$, so our claim is proved. Applying the result for $k = n-1$ we get $P_{n-1}(a) + \alpha_1 = b_{n-1}^l$ with $b_{n-1} \in \mathbb{F}_q(\alpha_1)$. This implies

$$\begin{aligned} N_{\mathbb{F}_q(\alpha_1)/\mathbb{F}_q}(P_{n-1}(a) + \alpha_1) &= N_{\mathbb{F}_q(\alpha_1)/\mathbb{F}_q}(\beta_1) \\ &= [N_{\mathbb{F}_q(\alpha_1)/\mathbb{F}_q}(b_{n-1})]^l \\ &= b_n^l \text{ with } b_n \in \mathbb{F}_q. \end{aligned}$$

Since $\alpha_1^d - a = 0$; then $[\beta_1 - P_{n-1}(a)]^d - a = 0$, hence

$$\begin{aligned} N_{\mathbb{F}_q(\alpha_1)/\mathbb{F}_q}(P_{n-1}(a) + \alpha_1) &= N_{\mathbb{F}_q(\alpha_1)/\mathbb{F}_q}(\beta_1) \\ &= (-1)^d \left\{ [-P_{n-1}(a)]^d - a \right\} \\ &= [P_{n-1}(a)]^d + (-1)^{d-1} a \\ &= P_n(a). \end{aligned}$$

Thus, $P_n(a) = b_n^l$ where $b_n \in \mathbb{F}_q$.

2. Suppose that $P_n(a) = 0$ for some $n \geq 2$; then $\Big(P_{n-1}(a)\Big)^d + (-1)^{d-1} a = 0$, hence $P_{n-1}(a)$ is a root of $x^d + (-1)^{d-1} a$ in $\mathbb{F}_q$. By Lemma 3.3 and item 3. of Corollary 3.6, we get $x^d - a$ is reducible over $\mathbb{F}_q$.

Suppose that for some $n \geq 1$, $P_n(a)$ is an *l-th* power in $\mathbb{F}_q^\star$ for some prime divisor l of d.

If $n = 1$, then according to Lemma 3.3, $f(x)$ is reducible over $\mathbb{F}_q$. Suppose that $n \geq 2$. We may suppose that $f_1(x), ..., f_{n-1}(x)$ are irreducible over $\mathbb{F}_q$. We have $P_n(a) = N_{\mathbb{F}_q(\alpha_1)/\mathbb{F}_q}(P_{n-1}(a) + \alpha_1)$, hence by Lemma 2.3, $P_{n-1}(a) + \alpha_1$ is an *l-th* power in $\mathbb{F}_q(\alpha_1)$. Suppose by induction that $P_{n-k}(a) + \alpha_k$ is an *l-th* power in $\mathbb{F}_q(\alpha_k)$. Since $P_{n-k}(a) + \alpha_k = N_{\mathbb{F}_q(\alpha_{k+1})/\mathbb{F}_q(\alpha_k)}(P_{n-(k+1)}(a) + \alpha_{k+1})$; then by Lemma 2.3 again , $P_{n-(k+1)}(a) + \alpha_{k+1}$ is an *l-th* power in $\mathbb{F}_q(\alpha_{k+1})$. In particular for $k = n-1$, we get that $P_1(a) + \alpha_{n-1}$ which is $a + \alpha_{n-1}$ is an *l-th* power in $\mathbb{F}_q(\alpha_{n-1})$. Since $\alpha_n^d - a - \alpha_{n-1} = 0$ then by Lemma 3.3, the polynomial $\alpha_n^d - (a + \alpha_{n-1})$ is reducible over $\mathbb{F}_q(\alpha_{n-1})$. Thus, $f_n(x)$ is reducible over $\mathbb{F}_q$ by Lemma 2.2. $\square$

For fixed $a \in \mathbb{F}_q^*$, the family $(P_n(a))_{n\geq 1}$ is finite. More precisely, let n_0 and m_0 be indices such that $n_0 < m_0$ and $P_{n_0}(a) = P_{m_0}(a)$. Suppose that n_0 first and m_0 next are chosen to be minimal with this property, then

$$\{P_n(a), n \geq 1\} = \{P_1(a), ..., P_{m_0-1}(a)\}\,. \tag{3}$$

Moreover, we have $m_0 \leq q+1$.

Theorem 4.2. *Let $d \geq 2$ be an integer such that $d \neq 0 \pmod 4$ and let $f(x) = x^d - a \in \mathbb{F}_q[x]$. Let n_0, m_0, with $n_0 < m_0$, be the minimal integers such that $P_{n_0}(a) = P_{m_0}(a)$. Then $f(x)$ is stable over $\mathbb{F}_q$ if and only if for any prime number $l \mid d$ and any $k \in \{1, ..., m_0 - 1\}$, $P_k(a) \notin \mathbb{F}_q^l$. Here $P_k(a) \notin \mathbb{F}_q^l$ means in particular $P_k(a) \neq 0$.*

Proof. If for some $l \mid d$ and some $k \in \{1, ..., m_0 - 1\}$, $P_k(a)$ is an l-th power, trivial or not; then by the preceding lemma, $f(x)$ is not stable. Conversely suppose that $f(x)$ is not stable over $\mathbb{F}_q$ and let n be the smallest positive integer such that $f_n(x)$ is reducible over $\mathbb{F}_q$. If $n = 1$, that is $f(x)$ is reducible, then $a = P_1(a)$ is an *l-th* power in $\mathbb{F}_q^\star$ for some prime divisor l of d. Suppose that $n \geq 2$, then by Lemma 4.1, there exists a prime number $l \mid d$ such that $P_n(a)$ is an *l-th* power in $\mathbb{F}_q^\star$. Since $P_n(a) = P_k(a)$ for some $k \in \{1, ..., m_0 - 1\}$, then $P_k(a)$ is an *l-th* power in $\mathbb{F}_q^\star$ as desired. □

Theorem 4.3. *Let $d \geq 2$ be an integer such that $d \neq 0 \pmod 4$ and let $f(x) = x^d - a \in \mathbb{F}_q[x]$ with $a \neq 0$. Suppose that $P_n(a)$ is an l-th power for some postive integer n and some prime number $l \mid d$. Let n_0 be the smallest positive integer satisfying this property. If $P_{n_0}(a) = 0$ or $n_0 = 1$ then $f(x)$ is reducible over $\mathbb{F}_q$. If $n_0 \geq 2$, then f_{n_0} is reducible while f_{n_0-1} is irreducible over $\mathbb{F}_q$. In any case $x^d - P_{n_0}(a)$ is reducible over $\mathbb{F}_q$.*

Proof. If $P_{n_0}(a) = 0$ or $n_0 = 1$ then, by the preceding lemma, $f(x)$ is reducible over $\mathbb{F}_q$. Supposing that $n_0 \geq 2$, the preceding lemma shows that $f_{n_0}(x)$ is reducible over $\mathbb{F}_q$. Since $f(x)$ is irreducible over $\mathbb{F}_q$ (otherwise $n_0 = 1$), then we may consider the greatest integer $m \in \{1, \ldots, n_0 - 1\}$ such that $f_m(x)$ is irreducible over $\mathbb{F}_q$, which in turn implies $f_{m+1}(x)$ is reducible over $\mathbb{F}_q$. Lemma 4.1 shows that $P_{m+1}(a)$ is an l-th power in $\mathbb{F}_q$. Since $m + 1 \leq n_0$ and n_0 is minimal, then $m + 1 = n_0$, hence $f_{n_0-1}(x)$ is irreducible over $\mathbb{F}_q$. The last statement is obvious and its proof will be omitted. □

Corollary 4.4. *Let $f(x) = x^d - a \in \mathbb{F}_q[x]$ with $a \neq 0$ and $d \not\equiv 0 \pmod 4$. Let δ be a positive integer such that $\delta \equiv 1 \pmod l$ for any prime factor l of d. Then $f(x)$ is stable over $\mathbb{F}_q$ if and only if it is stable over $\mathbb{F}_{q^\delta}$.*

Proof. It is not hard to see that the sufficiency of the condition follows.

Let us now prove that the condition in the hypothesis is necessary. By contradiction, suppose that $f(x)$ is not stable over $\mathbb{F}_{q^\delta}$. By Theorem 4.2, there exist an index n and a prime number $l \mid d$ such that $P_n(a) = 0$ or $P_n(a) \in \mathbb{F}_{q^\delta}^l$. In the first case $f(x)$ is not stable over $\mathbb{F}_q$, a contradiction. Now we consider the second possibility. Since $f(x)$ is stable over $\mathbb{F}_q$, then in particular $f(x)$ is irreducible, hence by item 1. of corollary 3.6, any prime factor of d divides $q-1$ thus, $l \mid q-1$. Now Lemma 2.1 implies $P_n(a) \in \mathbb{F}_q^l$ contradicting the stability of $f(x)$ over $\mathbb{F}_q$. $\square$

THEOREM 4.5. *Let $d \geq 2$ be an integer such that $d \neq 0 \pmod 4$ and let $f(x) = x^d - a \in \mathbb{F}_q[x]$ with $a \neq 0$. Let $\delta = gcd(q-1, d)$. Suppose that $P_n(a) \neq 0$ for any positive integer n. If $f_1(x), \dots, f_{(q-1)/\delta+1}(x)$ are irreducible over $\mathbb{F}_q$ then, $f(x)$ is stable.*

Proof. Let $H = \mathbb{F}_q^{\star(q-1)/\delta}$ and $A = \{P_1(a), \dots, P_{\frac{(q-1)}{\delta}+1}\}$. H is a subgroup of $\mathbb{F}_q^\star$, so its index is equal to $(q-1)/\delta$. Since the multiset A contains $\frac{(q-1)}{\delta}+1$ elements, there exist i and j with $i < j$ such that $P_j(a) \equiv P_i(a) \pmod H$, that is $P_j(a) = b^{(q-1/d)} P_i(a)$ with $b \in \mathbb{F}_q^\star$. Moreover, we may suppose that i and j are minimal with this property. This implies $P_j(a)^d = P_i(a)^d$ and then, by definition of the polynomials $P_k(x)$, $P_{j+1}(a) = P_{i+1}(a)$. From the definition of n_0 and m_0, we deduce that $i+1 = n_0$ and $j+1 = m_0$. Since $j \leq \frac{(q-1)}{\delta}+1$, then $m_0 - 1 = j \leq \frac{(q-1)}{\delta}+1$. Now the stability follows from Theorem 4.3. $\square$

REMARK 4.6. The preceding theorem shows that $m_0 \leq (q-1)/\delta + 2$. Here are two examples for which the bound is reached.

- $q = 7$, $d = 2$, $a = -2$, $\delta = 2$ and $f(x) = x^2 + 2$. We have $P_1(-2) = -2$, $P_2(-2) = -1$, $P_3(-2) = 3$, $P_4(-2) = -3$ and $P_5(-2) = -3$, hence $m_0 = 5 = (7-1)/2 + 2$.
- $q = 7$, $d = 3$, $a = 2$, $\delta = 3$ and $f(x) = x^2 - 2$. We have $P_1(2) = 2$, $P_2(2) = 3$, $P_3(2) = 1$ and $P_4(2) = 3$, hence $m_0 = 4 = (7-1)/3 + 2$.

COROLLARY 4.7. *Let $a \in \mathbb{F}_q^\star$. If d is odd, then $x^d - a$ is stable over $\mathbb{F}_q$ if and only if the same property holds for $x^d + a$*

Proof. By induction on n, we show that $P_n(-a) = -P_n(a)$. Then the conclusion follows immediately from the preceding theorem and from item 3. of Corollary 3.6. This identity is true by assumption. Suppose it is true for the step $n-1$. Then

$$P_n(-a) = \Big(P_{n-1}(-a)\Big)^d + (-a) = -\Big(P_{n-1}(a)\Big)^d - a = -P_n(a).$$

$\square$

REMARK 4.8. One verifies easily that

$$f_n(0) = \begin{cases} -P_n(a) \text{ for } n \geq 1 \text{ if } d \text{ is odd} \\ -P_1(a) \text{ if } n = 1 \text{ and } P_n(a) \text{ for } n \geq 2 \text{ if } d \text{ is even.} \end{cases}$$

Here we consider the case where the binomials are not monic.

Proposition 4.9. *Let $g(x) = bx^d - c \in \mathbb{F}_q[x]$, with b and $c \neq 0$. If some prime factor l of d does not divide $q-1$, then $g(x)$ is reducible over $\mathbb{F}_q$. Suppose that any prime factor of d divides $q-1$. Then there exist a and $\lambda \in \mathbb{F}_q^\star$ such that $g(x) = \big(u^{-1} \circ f \circ u\big)(x)$, where $u(x) = \lambda x$ and $f(x) = x^d - a$. Moreover, $g(x)$ is stable over $\mathbb{F}_q$ if and only if $f(x)$ is.*

Proof. If $l \mid d$ and $l \nmid q-1$, then $cb^{-1} \in \mathbb{F}_q^{\star l}$, hence $x^d - cb^{-1}$ is reducible over $\mathbb{F}_q$ and then the same holds for $g(x)$. Suppose that any prime factor of d divides $q-1$. The condition that there exist a and $\lambda \in \mathbb{F}_q^\star$ such that $g(x) = \big(u^{-1} \circ f \circ u\big)(x)$ is equivalent to $b = \lambda^{d-1}$ and $c = a\lambda^{-1}$. Since $gcd(d-1, q-1) = 1$, then the first equation determines λ. The second equation determines a. The statement about stability follows from Lemma 2.4

□

Example 4.10. 1. $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. So $a = -1$ and $d = 2$. $P_1(a) = P_2(a) = -1$. -1 is not a square in $\mathbb{F}_3$, hence $x^2 + 1$ is stable over $\mathbb{F}_3$.

2. $f(x) = x^2 - 2 \in \mathbb{F}_5[x]$. So $a = 2$ and $d = 2$. $P_1(a) = P_2(a) = 2$ which is not a square in $\mathbb{F}_5$, hence the stability of $x^2 - 2$ over $\mathbb{F}_5$.

3. $f(x) = x^2 + 2 \in \mathbb{F}_5[x]$. So $a = -2$ and $d = 2$. $P_1(a) = -2$ and $P_2(a) = 1$ which is a square in $\mathbb{F}_5$. $x^2 + 2$ is not stable over $\mathbb{F}_5$.

4. We have $\mathbb{F}_9 = \mathbb{F}_3(i)$ where $i^2 = -1$.

- $f_1(x) = x^2 - (1+i) \in \mathbb{F}_9[x]$.
  So $a = (1+i)$ and $d = 2$. $P_3(a) = -1$ which is a square in $\mathbb{F}_9$, hence $x^2 - (1+i)$ is not stable over $\mathbb{F}_9$.
- $f_2(x) = x^2 + (1+i) \in \mathbb{F}_9[x]$.
  So $a = -(1+i)$ and $d = 2$. $P_2(a) = 1$ which is a square in $\mathbb{F}_9$, hence $x^2 + (1+i)$ is not stable over $\mathbb{F}_9$.
- $f_3(x) = x^2 - (1-i) \in \mathbb{F}_9[x]$.
  So $a = 1 - i$ and $d = 2$. $P_3(a) = -1$ which is a square in $\mathbb{F}_9$, hence $x^2 - (1-i)$ is not stable over $\mathbb{F}_9$.
- $f_4(x) = x^2 - (i-1) \in \mathbb{F}_9[x]$.
  So $a = i - 1$ and $d = 2$. $P_2(a) = 1$ which is a square in $\mathbb{F}_9$, hence $x^2 - (i-1)$ is not stable over $\mathbb{F}_9$.

A Mersenne number is a positive integer of the form $2^m - 1$, where m is an integer at least equal to 2. Set $q = 2^m$. When $q-1$ is prime, this prime is called a Mersenne prime. It is well known that if $q-1$ is a Mersenne prime then m is prime. The converse is false, the first counterexample being $2^{11} - 1 = 2047 = 23 \times 89$. We prove the following.

Theorem 4.11.

1. *Let q be a non-trivial prime power and $\alpha \in \mathbb{F}_q^\star$. Then $x^{q-1} - \alpha$ is irreducible over $\mathbb{F}_q$ if and only if α generates $\mathbb{F}_q^\star$.*
2. *Suppose that $q = 2^m$, where $m \geq 2$ is an integer. Then the following conditions are equivalent.*

(i) *For any* $\alpha \in \mathbb{F}_q \setminus \{0,1\}$, $x^{q-1} - \alpha$ *is stable over* $\mathbb{F}_q$
(ii) *For any* $\alpha \in \mathbb{F}_q \setminus \{0,1\}$, $x^{q-1} - \alpha$ *is irreducible over* $\mathbb{F}_q$
(iii) $q-1$ *is a Mersenne prime.*

Proof.

1. **Necessity of the condition.** Let e be the order of α in $\mathbb{F}_q^\star$. Obviously $e \leq q-1$. On the other hand, let l be a prime divisor of $q-1$. Suppose, by contradiction, that the l-adic valuations satisfy the condition $\nu_l(a) < \nu_l(q-1)$; then $l \mid (q-1)/e$, which contradicts the irreducibility of $x^{q-1} - \alpha$ (see Lemma 3.4). Therefore, $\nu_l(a) = \nu_l(q-1)$, and then $e = q-1$.

   Sufficiency of the condition. Since $e = q-1$, then, by Lemma 3.4 , $x^{q-1} - \alpha$ is irreducible over $\mathbb{F}_q$.
2.
   - $(i) \Rightarrow (ii)$. Obvious.
   - $(ii) \Rightarrow (iii)$. By 1., for any $\alpha \in \mathbb{F}_q \setminus \{0,1\}$, α generates $\mathbb{F}_q^\star$. This implies that the order of this cyclic group is a prime number thus, $q-1$ is prime.
   - $(iii) \Rightarrow (i)$. By 1., for any $\alpha \in \mathbb{F}_q \setminus \{0,1\}$, $x^{q-1} - \alpha$ is irreducible over $\mathbb{F}_q$. To get the stability, since $(\mathbb{F}_q^\star)^{q-1} = \{1\}$, we must show that $P_n(\alpha) \notin \{0,1\}$ for any $n \geq 1$. For $n = 1$, this is proved above. Suppose, by induction, that it is true for $n \geq 1$. We have $P_{n+1}(\alpha) = P_n(\alpha)^{q-1} + (-1)^{q-2}\alpha = 1 + \alpha$. If $P_{n+1}(\alpha) = 0$ then, $\alpha = 1$. If $P_{n+1}(\alpha) = 1$ then, $\alpha = 0$. In both cases we reach a contradiction. Therefore, $x^{q-1} - \alpha$ is stable over $\mathbb{F}_q$.

□

In [7] a table of irreducible polynomials over $\mathbb{F}_q$, of degree d, for small q and small d is given. The following table lists the stable binomials $f(x) = x^d - a$ for $3 \leq q \leq 27$, $2 \leq d \leq 10$, $d \neq 0 \pmod 4$ and $a \in \mathbb{F}_q \setminus \{0,1\}$. The values of d for which there exists a prime number $l \mid d$ and $l \nmid q-1$ are omitted since in this case $f(x)$ is reducible over $\mathbb{F}_q$(see Corollary 3.6). The values of d which are congruent to 0 modulo 4 are also omitted. For given q, d and a, the table lists the sequence $[P_1(a)], \ldots, P_{m_0}(a)]$ (see the begining of section 4 for the definition of this sequence). One and only one of this list, say $P_n(a)$, is possibly underlined. This means that $P_n(a)$ is an l-th power for some prime divisor l of d and n is the smallest positive integer satisfying this property. This implies that n is the smallest positive integer such that $f_n(x)$ is reducible over $\mathbb{F}_q$. If no element is underlined then $f(x)$ is stable.

The elements of $\mathbb{F}_q \setminus \{0,1\}$ are enumerated in the following way. If $q = p$ is a prime number, then $a = 2, \ldots, p-1$. If $q = p^e$ with $e \geq 2$, then a generator α of $\mathbb{F}_q^\star$ is chosen and its minimal polynomial over $\mathbb{F}_p$, $M(x)$, is mentioned. In this case $a = \alpha, \ldots, \alpha^{q-2}$. If a binomial $f(x)$ of degree d is revealed to be stable over $\mathbb{F}_q$ by this table, then we have an infinite list of polynomials having the same property.

Table of stable polynomials

$q=3$		$q=4, M(X)=X^2+X+1$			
$\underline{d=2}$		$\underline{d=3}$		$\underline{d=9}$	
a	List	a	List	a	List
2	$[2,2]s.$	α	$[\alpha,\alpha^2,\alpha^2]s.$	α	$[\alpha,\alpha^2,\alpha^2]s.$
		α^2	$[\alpha^2,\alpha,\alpha]s.$	α^2	$[\alpha^2,\alpha,\alpha]s.$
$q=5$					
$\underline{d=2}$					
2	$[2,2]s.$	3	$[3,\underline{1},3]ns.$	4	$[\underline{4},2,0,1]ns.$
$q=7$					
$\underline{d=2}$		$\underline{d=3}$		$\underline{d=6}$	
2	$[\underline{2},2]s.$	2	$[2,3,\underline{1},3]s.$	2	$[\underline{2},6,6]s.$
3	$[3,6,5,\underline{1},5]s.$	3	$[3,2,4,4]s.$	3	$[3,5,5]s.$
4	$[\underline{4},5,0,3,5]ns.$	4	$[4,5,3,3]s.$	4	$[\underline{4},4]ns.$
5	$[5,6,3,\underline{4},4]ns.$	5	$[5,4,\underline{6},4]ns.$	5	$[5,3,3]s.$
6	$[6,\underline{2},5,2]ns.$	6	$[\underline{6},5,5]ns.$	6	$[\underline{6},2,2]ns.$
$q=7$		$q=8$, $M(X)=X^3+X+1$		$q=9$, $M(X)=X^2+2X+2$	
$\underline{d=9}$		$\underline{d=7}$		$\underline{d=2}$	
2	$[2,3,\underline{1},3]ns.$	α	$[\alpha,\alpha^3,\alpha^3]s.$	α	$[\alpha,\underline{1},\alpha^3,\alpha]ns.$
3	$[3,2,4,4]s.$	α^2	$[\alpha^2,\alpha^6,\alpha^6]s.$	α^2	$[\underline{\alpha^2},\alpha^3,\alpha^2]ns.$
4	$[4,5,3,3]s.$	α^3	$[\alpha^3,\alpha,\alpha]s.$	α^3	$[\alpha^3,\underline{1},\alpha,\alpha^5,\alpha^6]ns.$
5	$[5,4,\underline{6},4]ns.$	α^4	$[\alpha^4,\alpha^5,\alpha^5]s.$	α^4	$[\underline{\alpha^4},\alpha^4]ns.$
6	$[\underline{6},4,4]ns.$	α^5	$[\alpha^5,\alpha^4,\alpha^4]s..$	α^5	$[\alpha^5,\alpha^3,\underline{\alpha^4},\alpha^2,\alpha^7,\alpha^4]ns.$
		α^6	$[\alpha^6,\alpha^2,\alpha^2]s.$	α^6	$[\underline{\alpha^6},\alpha,\alpha^6]ns.$
				α^7	$[\alpha^7,\alpha,\underline{\alpha^4},\alpha^6,\alpha^5,\alpha^4]ns.$
$q=11$					
$\underline{d=2}$		$\underline{d=5}$		$\underline{d=10}$	
2	$[2,2]s.$	2	$[2,\underline{1},3,3]ns.$	2	$[2,\underline{10},10]ns.$
3	$[\underline{3},6,0,8,6]ns.$	3	$[3,4,4]s.$	3	$[\underline{3},9,9]ns.$
4	$[\underline{4},1,8,5,10,8]ns.$	4	$[4,5,5]s.$	4	$[\underline{4},8,8]ns.$
5	$[\underline{5},9,10,7,0,6,9]ns.$	5	$[5,6,4,6]s.$	5	$[\underline{5},7,7]ns.$
6	$[6,8,\underline{3},3]ns$	6	$[6,5,7,5]s.$	6	$[6,6]s.$
7	$[7,\underline{9},8,2,8]ns.$	7	$[7,6,6]s.$	7	$[7,\underline{9},8,2,8]ns.$
8	$[8,\underline{1},4,8]ns.$	8	$[8,7,7]s.$	8	$[8,\underline{4},4]ns.$
9	$[\underline{9},6,5,5]ns.$	9	$[9,\underline{10},8,8]ns.$	9	$[\underline{9},3,3]ns.$
10	$[10,2,\underline{5},4,6,4]ns.$	10	$[\underline{10},9,0,10]ns.$	10	$[\underline{10},2,2]ns.$
$q=13$					
$\underline{d=2}$		$\underline{d=3}$		$\underline{d=6}$	
2	$[2,2]s.$	2	$[2,10,\underline{1},3,3]ns.$	2	$[2,\underline{10},12,12]ns.$
3	$[\underline{3},6,7,7]ns.$	3	$[3,4,2,11,\underline{8},8]ns.$	3	$[\underline{3},11,9,11]ns.$

4	$[\underline{4}, 12, 10, 5, 8, 8]ns.$	4	$[4, 3, \underline{5}, 12, 3]ns.$	4	$[\underline{4}, 10, 10]ns.$
5	$[5, 7, 5]s.$	5	$[\underline{5}, 0, 5]ns.$	5	$[\underline{5}, 7, 7]ns.$
6	$[6, \underline{4}, 10, 3, 3]ns.$	6	$[6, \underline{1}, 7, 1]ns.$	6	$[6, 6]s.$
7	$[7, \underline{3}, 2, 10, 2]ns.$	7	$[7, \underline{12}, 6, 2, 2]ns.$	7	$[7, \underline{5}, 5]ns.$
8	$[8, \underline{4}, 8]ns.$	8	$[\underline{8}, 0, 8]ns.$	8	$[\underline{8}, 4, 6, 4]ns.$
9	$[\underline{9}, 7, 1, 5, 3, 0, 4, 7]ns.$	9	$[9, 10, \underline{8}, 1, 10]ns.$	9	$[\underline{9}, 5, 3, 5]ns.$
10	$[10, 12, 4, 6, 0, 3, 12]ns.$	10	$[10, 9, 11, \underline{1}, 11]ns.$	10	$[\underline{10}, 4, 4]ns.$
11	$[11, 6, \underline{12}, 3, 11]ns.$	11	$[11, 3, \underline{12}, 10, 10]ns.$	11	$[11, \underline{1}, 3, 3]ns.$
12	$[\underline{12}, 2, 5, 0, 1, 2]ns.$	12	$[\underline{12}, 11, 4, 11]ns.$	12	$[\underline{12}, 2, 0, 2]ns.$
$q = 13$					
$\underline{d = 9}$					
2	$[2, 7, 10, \underline{1}, 3, 3]ns.$	3	$[3, 4, 2, 8, 11, 11]ns.$	4	$[4, 3, \underline{5}, 9, 5]ns.$
5	$[\underline{5}, 10, 4, 4]ns.$	6	$[6, 11, \underline{1}, 7, 1]ns.$	7	$[7, 2, \underline{12}, 6, 12]ns.$
8	$[\underline{8}, 3, 9, 9]ns.$	9	$[9, 10, \underline{8}, 4, 8]ns.$	10	$[10, 9, 11, \underline{5}, 2, 2]ns.$
11	$[11, 6, 3, \underline{12}, 10, 10]ns.$	12	$[\underline{12}, 11, 7, 7]ns.$		
$q = 16, M(x) = X^4 + X + 1$					
$d = 9$					
α	$[\alpha, \underline{\alpha^3}, \alpha^{13}, \alpha^{13}]ns.$	α^2	$[\alpha^2, \underline{\alpha^6}, \alpha^{11}, \alpha^{11}]ns.$	α^3	$[\underline{\alpha^3}, \alpha^{10}, \alpha^{14}, \alpha^2, . \; 0, \alpha^3]$ns.
α^4 .	$[\alpha^4, \underline{\alpha}^{12}, \alpha^7, \alpha^{11}, . \; \alpha^{14}, \alpha^{12}]$ns.	α^5	$[\alpha^5, \alpha^{10}, \alpha^{10}]s.$	α^6	$[\underline{\alpha^6}, \alpha^5, \alpha^{13}, \alpha^4, 0, \alpha^6]$ns
α^7	$[\alpha^7, \alpha^4, \alpha^{10}, \underline{\alpha^9}, \alpha^{10}]$ns.	α^8	$[\alpha^8, \underline{\alpha^9}, \alpha^{14}, \alpha^{14}]ns.$	α^9	$[\underline{\alpha^9}, \alpha^5, \alpha^7, \alpha, 0, \alpha^9]$ns.
α^{10}	$[\alpha^{10}, \alpha^5, \alpha^5]s.$	α^{11}	$[\alpha^{11}, \alpha^2, \alpha^5, \underline{\alpha^{12}}, \alpha^5]$ns	α^{12}	$[\underline{\alpha^{12}}, \alpha^{10}, \alpha^{11}, \alpha^8, 0, \alpha^{12}]$ns
α^{13}	$[\alpha^{13}\alpha, \alpha^{10}, \underline{\alpha^6}, \alpha^{10}]ns.$	α^{14}	$[\alpha^{14}, \underline{1}, \alpha^6, \alpha^{10}, \alpha^6]ns.$		
$q = 17$					
$d = 2$					
2	$[\underline{2}, 2]ns.$	3	$[3, 6, \underline{16}, 15, 1, 15]ns.$	4	$[\underline{4}, 12, 4]ns.$
5	$[5, 3, \underline{4}, 11, 14, 13, 4]ns.$	6	$[6, \underline{13}, 10, 9, 7, 9]ns.$	7	$[7, \underline{8}, 6, 12, 1, 11, 12]ns.$
8	$[\underline{8}, 5, 0, 9, 5]ns.$	9	$[\underline{9}, 4, 7, 6, 10, 6]ns.$	10	$[10, 5, \underline{15}, 11, 9, 3, 16, 3\ ]$ns
11	$[11, \underline{8}, 2, 10, 4, 5, 14, 15, 10]ns.$	12	$[12, \underline{13}, 4, 4]ns.$	13	$[\underline{13}, 3, 13]ns.$
14	$[14, 12, 11, 5, 11]s.$	15	$[\underline{15}, 6, 4, 1, 3, 11, 4]ns.$	16	$[\underline{16}, 2, 6, 4, 1, 2]ns.$
$q = 19$					
$d = 2$					
2	$[2, 2]s.$	3	$[3, \underline{6}, 14, 3]ns.$	4	$[\underline{4}, 12, 7, 7]ns.$
5	$[\underline{5}, 1, 15, 11, 2, 18, 15]$ns	6	$[\underline{6}, 11, 1, 14, 0, 13, 11]ns.$	7	$[\underline{7}, 4, 9, 17, 16, 2, 16]$ ns
8	$[8, 18, 12, 3, \underline{1}, 12]ns.$	9	$[\underline{9}, 15, 7, 2, 14, 16, 0, 10, 15]ns.$	10	$[10, 14, 15, \underline{6}, 7, 1, 10]ns.$

12	$[12, 18, 8, 14, 13, \underline{5}, 13]$	11	$[\underline{11}, 15, 5, 14, 14]ns.$	13	$[13, \underline{4}, 3, 15, 3]ns.$
14	$[14, \underline{11}, 12, 16, , 14]$ ns.	15	$[15, \underline{1}, 5, 10, 9, 9]ns.$	16	$[\underline{16}, 12, 14, 9, 8, 10, . 8]ns.$
17	$[\underline{17}, 6, 0, 2]ns.$	18	$[18, 2, \underline{5}, 7, 12, 12]ns.$		
$\underline{d = 3}$		$\underline{d = 6}$		$\underline{d = 9}$	
2	$[2, 10, 14, 10]s.$	2	$[2, \underline{5}, 5]ns.$	2	$[2, \underline{1}, 3, 1]ns.$
3	$[3, \underline{11}, 4, 10, 15, 15]ns.$	3	$[3, \underline{4}, 8, 17, 8]ns.$	3	$[3, 2, 2]s.$
4	$[4, \underline{11}, 5, 15, 16, 15]ns.$	4	$[\underline{4}, 7, 0, 15, 7]ns$	4	$[4, 5, 5]s.$
5	$[5, 16, 16]s.$	5	$[\underline{5}, 2, 2]ns.$	5	$[5, 6, 6]s.$
6	$[6, 13, \underline{18}, 5, 17, 17]$	6	$[\underline{6}, 5, 1, 14, 1]ns.$	6	$[6, \underline{7}, 7]ns.$
7	$[\underline{7}, 8, 6, 14, 15, 0, 7]ns.$	7	$[\underline{7}, 16, 0, 8, 8]ns$	7	$[\underline{7}, 8, 8]ns.$
8	$[\underline{8}, 7, 9, 15, 1, 9]ns.$	8	$[\underline{8}, 7, 15, 3, 18, 12$	8	$[\underline{8}, 9, 9]ns.$
9	$[9, 16, \underline{1}, 19, 2, 17, 1]ns.$	9	$[\underline{9}, 2, 17, 17]ns.$	9	$[9, 10, \underline{8}, 8]ns.$
10	$[10, 3, \underline{18}, 9, 17, 2, . 18]ns.$	10	$[10, \underline{1}, 10]ns$	10	$[10, 9, \underline{11}, 11]ns.$
11	$[\underline{11}, 12, 10, 4, 18, 10]ns.$	11	$[\underline{11}, 9, 0, 8, 9]ns.$	11	$[\underline{11}, 10, 10]ns.$
12	$[\underline{12}, 11, 13, 5, 4, 0, 12]ns.$	12	$[\underline{12}, 11, 8, 8]ns.$	12	$[\underline{12}, 11, 11]ns.$
13	$[13, 6, \underline{1}, 14, 5, 14]ns.$	13	$[13, \underline{17}, 13]ns.$	13	$[13, \underline{12}, 12]ns.$
14	$[14, 3, 3]s.$	14	$[14, \underline{12}, 6, 16, 12]ns.$	14	$[14, 13, 13]s.$
15	$[15, \underline{8}, 14, 4, 3, 4]ns.$	15	$[15, 15]s.$	15	$[15, 14, 14]s.$
16	$[16, 4, 4]s.$	16	$[\underline{16}, 10, 14, 10]ns.$	16	$[16, \underline{11}, 4, 10, 15, 15]$ $ns.$
17	$[17, 9, 5, 9]s.$	17	$[\underline{17}, 9, 13, 13]ns.$	17	$[17, \underline{18}, 16, 18]ns.$
18	$[\underline{18}, 17, 10, 11, 0, 18]ns.$	18	$[\underline{18}, 2, 8, 2]ns.$	18	$[\underline{18}, 17, 0, 18]ns.$
$q = 23$					
$\underline{d = 2}$					
2	$[\underline{2}, 2]ns.$	3	$[\underline{3}, 6, 10, 5, 22, 21, 1, 21]ns.$	4	$[\underline{4}, 12, 2, 0, 19, 12]ns.$
5	$[5, 20, 4, 11, \underline{1}, 19, 11]ns.$	6	$[\underline{6}, 7, 20, 3, 3]ns.$	7	$[7, 19, \underline{9}, 5, 18, 18]ns.$
8	$[\underline{8}, 10, 0, 15, 10]ns.$	9	$[\underline{9}, 3, 0, 14, 3]ns.$	10	$[10, 21, 17, \underline{3}, 22, 14, 2, 17]ns.$
11	$[11, \underline{18}, 14, 1, 13, 20, 21, 16,]$	12	$[\underline{12}, 17, 1, 12]ns.$	13	$[\underline{13}, 18, 12, 15, 13]ns.$
14	$[14, 21, \underline{13}, 17, 22, 10, . 20, 17]ns.$	15	$[15, 3, 17, 21, \underline{12}, 14,$	16	$[\underline{16}, 10, 15, 2, 11, 13, 15$]ns
17	$[17, 19, 22, 7, \underline{9}, 18, 8, 1, 7]ns.$	18	$[\underline{18}, 7, 8, 0, 5, 7]ns.$	19	$[19, 20, \underline{13}, 12, 10, 12$]ns
20	$[20, \underline{12}, 9, 15, 21, 7, 6, 16, 6]$ns	21	$[21, \underline{6}, 15, 20, 11, 8, 20]ns.$	22	$[22, \underline{2}, 5, 3, 9, 13, 9]ns.$

$q=25, M(X)=X^2+4X+2$					
	$\underline{d=2}$		$\underline{d=3}$		$\underline{d=6}$
α	$[\alpha,\underline{\alpha^{18}},\alpha^{10},\alpha^{21},\alpha^3,\alpha^{14},\alpha^{15},\alpha^{14}]ns.$	α	$[\alpha,\underline{\alpha^{18}},\alpha^{15},\alpha^{20},\alpha^{17},\alpha^{18}]ns$	α	$[\alpha,\underline{\alpha^{14}},\alpha^5,\alpha^{14}]ns.$
α^2	$[\underline{\alpha^2},\alpha^{17},\alpha^9,\alpha,0,\alpha^{14},\alpha^{17}]\text{ns.}$	α^2	$[\alpha^2,\alpha,\underline{1},\alpha^{17},1]ns.$	α^2	$[\underline{\alpha^2},\alpha^5,\alpha^{10}\alpha^5]ns.$
α^3	$[\alpha^3,\alpha^{17},\underline{1},\alpha^2,\alpha^{20},\alpha^{13},\alpha^7,\alpha^{12},\alpha^2]ns.$	α^3	$[\underline{\alpha^3},\alpha^{21,0,\alpha^3}]ns.$	α^3	$[\underline{\alpha^3},\alpha,\alpha^{17},\alpha^{17}]ns.$
α^4	$[\underline{\alpha^4},\alpha^{12},\alpha^{20},\alpha^{22},\alpha^{15},\alpha^{19},\alpha^7,\alpha^7]ns.$	α^4	$[\alpha^4,\alpha^8,\alpha^{23},\alpha^5,\alpha^{20}\ \alpha^8]s.$	α^4	$[\underline{\alpha^4},\alpha^{20},\alpha^{20}]ns.$
α^5	$[\alpha^5,\underline{\alpha^{18}},\alpha^2,\alpha^9,\alpha^{15},\alpha^{22},\alpha^5.\alpha^9,]ns.$		$[\alpha^5,\underline{\alpha^{18}},\alpha^3,\alpha^4,\alpha^{13},\alpha^{18}]ns.$	α^5	$[\alpha^5,\_\alpha^{22},\alpha^2,\alpha^2]ns.$
α^6	$[\underline{\alpha^6},\alpha^6]ns.$	α^6	$[\underline{\alpha^6},0,\alpha^6]ns.$	α^6	$[\underline{\alpha^6},\alpha^6]ns.$
α^7	$[\alpha^7,\underline{\alpha^4},\alpha^{24},\alpha^9,\alpha^{16},\alpha^{24}]ns.$	α^7	$[\alpha^7,\alpha^{10},\alpha^4,\underline{\alpha}^{21},\alpha^{11},\alpha^{24},\alpha^8,\alpha^8]ns.$	α^7	$[\alpha^7,\underline{\alpha^{16}},\alpha^9,\alpha^{11}\alpha^{16}]\ ns.$
α^8	$[\underline{\alpha^8},\alpha^{15},\alpha^9,\alpha^{13},\alpha^{14},\alpha^{24}]$	α^8	$[\alpha^8,\alpha^4,\alpha^7,\alpha^{13},\alpha^{16},\alpha^4]s.$	α^8	$[\underline{\alpha^8},\alpha^{19},\alpha^{11},\alpha^{11}]ns.$
α^9	$[\alpha^9,\underline{\alpha^4},\alpha^{13},\alpha^{11},\alpha^{19},\alpha^{22}]$	α^9	$[\underline{\alpha^9},\alpha^{21},\alpha^3,\alpha^{21}]ns.$	α^9	$[\underline{\alpha^9},\alpha^8,\alpha^7,\alpha^4,\alpha^7]ns.$
α^{10}	$[\underline{\alpha^{10}},\alpha^{13},\alpha^8,\alpha^{10}]ns.$	α^{10}	$[\alpha^{10},\alpha^5,\underline{1},\alpha^{13},\alpha^{24}]ns.$	α^{10}	$[\underline{\alpha^{10}},\alpha,\alpha^2,\alpha]ns.$
α^{11}	$[\alpha^{11},\underline{\alpha^{20}},\alpha^{24},\alpha^8,\alpha^{24}]$	α^{11}	$[\alpha^{11},\alpha^2,\alpha^{20},\underline{\alpha^9},\alpha^7,\alpha^{24},\alpha^{16},\alpha^{16}]ns.$	α^{11}	$[\alpha^{11},\underline{\alpha^8},\alpha^{21},\alpha^7,\alpha^8]\ ns.$
α^{12}	$[\underline{\alpha^{12}},\alpha^6,0,\alpha^{24},\alpha^6]ns$	α^{12}	$[\underline{\alpha^{12}},\alpha^{18},\alpha^{24},\alpha^{12}]ns.$	α^{12}	$[\underline{\alpha^{12}},\alpha^6,0,\alpha^{24},\alpha^6]ns.$
α^{13}	$[\alpha^{13},\alpha^{23},\underline{\alpha^8},\alpha^3,\alpha^{15}]ns$	α^{13}	$[\alpha^{13},\underline{\alpha^6},\alpha^3,\alpha^8,\alpha^5]$	α^{13}	$[\alpha^{13},\underline{\alpha^{15}},\alpha^2,\alpha^{17},\alpha^{15}]ns.$
α^{15}	$[\alpha^{15},\alpha^{13},\underline{1},\alpha^{10}\ \alpha^4,\alpha^{17}]ns$	α^{15}	$[\underline{\alpha^{15}},\alpha^9,0,\alpha^{15}]ns.$	α^{15}	$[\underline{\alpha^{15}},\alpha^5,\alpha^{13},\alpha^{13}]ns.$
α^{16}	$[\underline{\alpha^{16}},\alpha^3,\alpha^{21},\alpha^7,\alpha^{17},\alpha^{22}].$	α^{16}	$[\alpha^{16},\alpha^{20},\alpha^{11},\alpha^{17},\alpha^8,\alpha^{20}]s$	α^{16}	$[\underline{\alpha^{16}},\alpha^{23},\alpha^7,\alpha^7]ns.$
α^{17}	$[\alpha^{17},\alpha^{19},\underline{\alpha^{16}},\alpha^{15},\alpha^3,]ns$	α^{17}	$[\alpha^{17},\underline{\alpha^6},\alpha^{15},\alpha^{16},\alpha,\alpha^6]ns$	α^{17}	$[\alpha^{17},\underline{\alpha^3},\alpha^{10},\alpha^{13},\alpha^3]ns.$
α^{18}	$[\alpha^{18},1,\alpha^{18}]ns.$	α^{18}	$[\underline{\alpha^{18}},0,\alpha^{18}]ns.$	α^{18}	$[\underline{\alpha^{18}},\alpha^{24},\alpha^{18}]ns.$
α^{19}	$[\alpha^{19},\alpha^{15},\underline{\alpha^4},\alpha^5,\alpha^{17},$	α^{19}	$[\alpha^{19},\alpha^{22};\alpha^{16};\alpha^{19};\alpha^9]\text{ns.}$	α^{19}	$[\alpha^{19},\alpha^{23},\alpha^{23}]s.$
α^{20}	$[\underline{\alpha^{20}},\alpha^{12},\alpha^4,\alpha^{14},\alpha^3,\alpha^{23}]$	α^{20}	$[\alpha^{20}\alpha^{16},\alpha^{19},\alpha,\alpha^4,\alpha^{16}]s.$	α^{20}	$[\underline{\alpha^{20}}\alpha^4,\alpha^4]ns.$
α^{21}	$[\underline{\alpha^{21}},\alpha^{16},\alpha^{11},\alpha^{20},\alpha^{11}]ns.$	α^{21}	$[\underline{\alpha^{21}},\alpha^3,\alpha^{15},\alpha^9,0,\alpha^{21}]ns.$	α^{21}	$[\alpha^{21},\alpha^{23},\underline{\alpha^{10}},\alpha^{10}]ns.$
α^{22}	$[\underline{\alpha^{22}},\alpha^{23},0,\alpha^{10},\alpha^{23}]\text{ns.}$	α^{22}	$[\alpha^{22},\alpha^{17},\underline{\alpha^{12}},\alpha,\alpha^{12}]ns.$	α^{22}	$[\underline{\alpha^{22}},\alpha^3,\alpha^{14},\alpha^3]ns.$
α^{23}	$[\alpha^{23},\alpha^3,\underline{\alpha^{20}},\alpha,\alpha^{13},\alpha^{13}]ns.$	α^{23}	$[\alpha^{23},\alpha^{14},\alpha^8,\underline{\alpha^{21}},\alpha^{19},\alpha^{12},\alpha^4,\alpha^4]$	α^{23}	$[\alpha^{23},\alpha^{19},\alpha^{19}]s.$

$q=25, M(X)=X^2+4X+2$					
			$\underline{d=9}$		
α	$[\alpha,\alpha^5,\alpha]s.$	α^9	$[\underline{\alpha^9},\alpha^{15},\alpha^3,\alpha^{23},\alpha^3]ns.$	α^{17}	$[\alpha^{17},\alpha^7,\alpha^8,\alpha,\alpha^7]s.$
α^2	$[\alpha^2,\alpha,\alpha^{10},\alpha]s.$	α^{10}	$[\alpha^{10},\alpha^{14},\alpha^5,\alpha^2,\alpha^{14}]s.$	α^{18}	$[\underline{\alpha^{18}},\alpha^{24},\alpha^{12},\alpha^6,0,\alpha^{18}]ns.$

α^3	$[\underline{\alpha^3},\alpha^9,\alpha^{21},\alpha^{15},0,\alpha^3]ns.$	α^{11}	$[\alpha^{11},\alpha^7,\alpha^{10},\alpha^{19},\alpha^7]s.$	α^{19}	$[\alpha^{19},\alpha^{23},\alpha^{14},\alpha^{11},\alpha^{23}]s.$
α^4	$[\alpha^4,\alpha^8,\alpha^{23},\alpha^{20},\alpha^8]s.$	α^{12}	$[\underline{\alpha^{12}},\alpha^{18},\alpha^6,\alpha^{24},0,\alpha^{12}]ns.$	α^{20}	$[\alpha^{20},\alpha^{16},\alpha^{19},\alpha^4,\alpha^{16}]s.$
α^5	$[\alpha^5,\alpha,\alpha^4,\alpha^{13},\alpha]s.$	α^{13}	$[\alpha^{13},\alpha 17,\alpha^8,\alpha^5,\alpha^{17}]s.$	α^{21}	$[\underline{\alpha^{21}},\alpha^3,\alpha^{15},\alpha^9,0,\alpha^{21}]ns.$
α^6	$[\alpha^6,\alpha^{12},\alpha^{24},\alpha^{18},0,\alpha^6]$	α^{14}	$[\alpha^{14},\alpha^{10},\alpha^{13},\underline{\alpha^{12}},\alpha^{10}]ns.$	α^{22}	$[\alpha^{22},\alpha^2,\alpha^{17},\alpha^{14},\alpha^2]s.$
α^7	$[\alpha^7,\alpha^{11},\alpha^2,\alpha^{23},\alpha^{11}]s.$	α^{15}	$[\underline{\alpha^{15}},\alpha^{21},\alpha^9,\alpha^3,0,\alpha^{15}]ns.$		
α^8	$[\alpha^8,\alpha^4,\alpha^7,\alpha^{16},\alpha^4]s.$	α^{16}	$[\alpha^{16},\alpha^{20},\alpha^{11},\alpha^8,\alpha^{20}]s.$		
$q=27,\ M(X)=X^3+X+1$					
$\underline{d=2}$					
α	$[\alpha,\underline{\alpha^4},\alpha^{13},\alpha^7,\alpha]ns.$	α^{10}	$[\underline{\alpha^{10}},\alpha^{21},\alpha^{20},\alpha^{17},\alpha^7,\alpha^{17}]ns$	α^{18}	$[\underline{\alpha^{18}},\alpha^{22},0,\alpha^5,\alpha^{12}]ns.$
α^2	$[\underline{\alpha^2},\alpha^{14},0,\alpha^{15},\alpha^{14}]ns.$	α^{11}	$[\alpha^{11},\alpha^{17},\underline{\alpha^4},\alpha^4]ns.$	α^{19}	$[\alpha^{19},\alpha^{17},\alpha,\underline{\alpha^{20}},\alpha^{21},\alpha^{12},\alpha^{13},\alpha^{11},\alpha^2,\alpha^{25},\alpha^{13}]ns.$
α^3	$[\alpha^3,\underline{\alpha^{12}},\alpha^5,\alpha^{21},\alpha^3]ns.$	α^{12}	$[\underline{\alpha^{12}},\alpha^7,\alpha^7]ns.$	α^{20}	$[\underline{\alpha^{20}},\alpha^{11},\alpha^6,\alpha^{24},\alpha^6]ns.$
α^4	$[\underline{\alpha^4},\alpha^{11},\alpha^8,\alpha^{25},\alpha^{21},\alpha^{25}]ns$	α^{13}	$[\alpha^{13},\alpha^{13}]s.$	α^{21}	$[\alpha^{21},\alpha^{23},\underline{\alpha^{10}},\alpha^{10}]ns.$
α^5	$[\alpha^5,\alpha^{25},\alpha^3,\underline{\alpha^8},\alpha^{11},\alpha^{10},\alpha^4,\alpha^{14},\alpha^{24},\alpha^{10}]ns.$	α^{14}	$[\underline{\alpha^{14}},\alpha^{10},\alpha^{24},\alpha^9,\alpha^{21},1,\alpha^9,]ns.$	α^{22}	$[\underline{\alpha^{22}},\alpha^{12},\alpha^8,\alpha^{13},\alpha^3,\alpha^7,\alpha^3]ns.$
α^6	$[\underline{\alpha^6},\alpha^{16},0,\alpha^{19},\alpha^{16}]ns.$	α^{15}	$[\alpha^{15},\alpha^{23},\alpha^9,\underline{\alpha^{24}},\alpha^7,\alpha^4,\alpha^{13},\alpha^{21},\alpha^{18},\alpha^{17},\alpha^{13}]ns.$	α^{23}	$[\alpha^{23},\underline{\alpha^{16}},\alpha^{24},\alpha^{12},1,\alpha^6,\alpha^5,\alpha^{23}]ns.$
α^7	$[\alpha^7,\alpha^{25},\alpha^{12},\underline{\alpha^{12}}]ns.$	α^{16}	$[\underline{\alpha^{16}},\alpha^4,\alpha^{20},\alpha^{13},\alpha,\alpha^{11},1,\alpha]ns.$	α^{24}	$[\underline{\alpha^{24}},\alpha^{21},\alpha^2,\alpha^8,\alpha^2]ns.$
α^8	$[\underline{\alpha^8},\alpha^7,\alpha^{18},\alpha^{20},\alpha^{18}]ns.$	α^{17}	$[\alpha^{17},\underline{\alpha^{22}},\alpha^{20},\alpha^{10},1,\alpha^{18},\alpha^{15},\alpha^{17}]ns.$	α^{25}	$[\alpha^{25},\underline{\alpha^{14}},\alpha^8,\alpha^4,1,\alpha^2,\alpha^{19},\alpha^{25}]ns.$
$\alpha^9.$	$[\alpha^9,\underline{\alpha^{10}},\alpha^{15},\alpha^{11},\alpha^9]ns.$				

REFERENCES

[1] O. Ahmadi and K. Monsef-Shokri, *A note on the stability of trinomials over finite fields*, Finite Fields Appl., **63** (2020), Article 101649, 1–13.

[2] N. Ali, *Stabilité des polynômes*, Acta Arith., **119** (2005), 53–63.

[3] M. Ayad and D. L. McQuillan, *Irreducibility of the iterates of a quadratic polynomial over a field*, Acta Arith., **93** (2000), 87–97.

[4] M. Ayad and D. L. McQuillan, *Corrections to "Irreducibility of the iterates of a quadratic polynomial over a field"*, Acta Arith., **99** (2001), 97–97.

[5] L. Danielson and B. Fein, *On the irreducibility of the iterates of* $x^n - b$, Proc. Amer. Math. Soc., **130** (2001), 1589–1596.

[6] Serge Lang, *Algebra*, Addison-Wesley, 1965.

[7] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1986.

[8] R. W. K. Odoni, *On the prime divisors of the sequence* $w_{n+1} = 1 + w_1 \cdots w_n$, J. London Math. Soc., **32** (1985), 1–11.

[9] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc., **51** (1985), 385–414.

[10] N. G. Tchebotarow, *Grundzuge der Galois'schen Theorie (translated from Russian by H. Schwerdtfeger)*, Noordhoff, Groningen, 1950.

Received December 17, 2022
Accepted September 14, 2023

Université du Littoral
Laboratoire LMPA, F-62228 Calais. France
E-mail: ayadmohamed502@yahoo.com
https://orcid.org/0000-0002-9400-6408

USHTB
Laboratoire LA3C, Alger, Algérie
E-mail: b.benseba@usthb.dz
https://orcid.org/0000-0002-5760-8100
E-mail: mo7amadi@outlook.com