Noname manuscript No.
(will be inserted by the editor)

Swan-like results for binomials and trinomials over finite fields of odd characteristic

B. Hanson · D. Panario · D. Thomson

the date of receipt and acceptance should be inserted later

Abstract Swan (1962) gives conditions under which the trinomial $x^n + x^k + 1$ over $\mathbb{F}_2$ is reducible. Vishne (1997) extends this result to trinomials over extensions of $\mathbb{F}_2$. In this work we determine the parity of the number of irreducible factors of all binomials and some trinomials over the finite field $\mathbb{F}_q$, where q is a power of an odd prime.

Keywords Irreducible polynomials · Swan's Theorem · Discriminant · Finite fields

Mathematics Subject Classification (2000) 11T06 · 12Y05

1 Introduction

Irreducible polynomials with few nonzero terms are important in efficient applications of digital communications systems such as coding theory, cryptography and signal processing. Trinomials and pentanomials, polynomials with three and five non-zero terms, respectively, over $\mathbb{F}_2$ have been studied in this context. In general, it is unknown when a polynomial with a given number of non-zero terms is irreducible. Therefore, results characterizing the irreducibility of such polynomials are important. Swan [14] gave the first result on the reducibility of such polynomials over finite fields.

Swan's theorem gives the parity of the number of irreducible factors of trinomials over $\mathbb{F}_2$. Swan relies on a result which relates the discriminant of a polynomial with its number of irreducible factors. This result was originally

B. Hanson
Department of Mathematics, University of Toronto, Room 6290, 40 St. George St., Toronto ON, M5S 2E4. E-mail: brandon.hanson@utoronto.ca

D. Panario · D. Thomson
School of Mathematics and Statistics, Carleton University, 1125 Colonel By Dr., Ottawa ON, K1S 5B6. E-mail: {daniel, dthomson}@math.carleton.ca

given by Pellet [12] for prime fields, and later by Stickelberger [13] for general p-adic fields. As a corollary, Swan proves that there is no irreducible trinomial over $\mathbb{F}_2$ of degree $8k$, where k is any positive integer [14]. Swan's theorem has recently been used by Brent and Zimmerman [3] to reduce the number of cases in a search for primitive trinomials over $\mathbb{F}_2$ of enormous degree.

Many results similar to Swan's theorem concentrate on determining the reducibility of polynomials over $\mathbb{F}_2$. Hales and Newhart [5] give a Swan-like result for binary tetranomials. Bluher [2] gives a Swan-like theorem for binary polynomials of the form $x^n + \sum_{i \in S} x^i + 1$, where $S \subset \{i : i \text{ odd}, 0 < i < n/3\} \bigcup \{i : i \equiv n \pmod 4, 0 < i < n\}$. Zhao and Cao [16] show that all binary affine polynomials are reducible except for x^2+x+1 and x^4+x+1. Koepf and Kim [7] give a Swan-like result for the so-called Type II binary pentanomials.

Some recent work has been conducted on the reducibility of polynomials over finite fields of odd characteristic. Von zur Gathen [4] shows that a polynomial over $\mathbb{F}_q$, q odd, being squarefree with an odd number of irreducible factors depends only on the values of $n \pmod{m_1}, k \pmod{m_2}$ and $k/\gcd(n,k) \pmod{q-1}$, where $m_2 = p(q-1)$ and $m_1 = \operatorname{lcm}(4, m_2)$. He then analyzes the special case of trinomials over $\mathbb{F}_3$ and gives a table of conditions for which a trinomial over $\mathbb{F}_3$ is squarefree and has an odd number of irreducible factors. In this work, von zur Gathen poses some conjectures on the distribution of irreducible trinomials over $\mathbb{F}_3$. One of these conjectures was proven by Ahmadi, see [1]. Kim and Koepf [6] examine the parity of the number of the irreducible factors of compositions of some polynomials over finite fields of odd characteristic. Loidreau [10] gives the parity of the number of irreducible factors for any trinomial over $\mathbb{F}_3$ by examining the discriminant using all possible congruences of n and $k \pmod{12}$. This type of analysis holds for higher characteristic, but the number of cases grows quickly with the characteristic, making a complete analysis for large q hard to achieve.

Sufficient and necessary conditions on the irreducibility of binomials over finite fields $\mathbb{F}_q$ are well known, see [9, Theorem 3.75]. However, these results require the factorization of $q-1$. In this paper, we give a complete characterization of the parity of the number of irreducible factors of binomials over $\mathbb{F}_q$, q odd, that does not require the factorization of $q-1$. We also give a partial result on the reducibility of trinomials over $\mathbb{F}_q$. Several cases are not covered as they depend on unknown properties of the quadratic character. We consider only monic polynomials with non-zero constant term. Thus, we denote these binomials as $x^n + a \in \mathbb{F}_q[x]$, $a \neq 0$, and the trinomials as $x^n + ax^k + b \in \mathbb{F}_q[x]$, $ab \neq 0$.

The structure of the paper is as follows: in Section 2 we present some background and preliminary results to give the parity of the number of irreducible factors of polynomials over finite fields. In Section 3 we give conditions for completely determining the parity of the number of irreducible factors of binomials over finite fields. In Section 4 we give conditions to determine the parity of the number of irreducible factors of certain classes of trinomials over finite fields. Then, in Section 5 we give Swan-like reducibility conditions for some

other classes of polynomials for which the method in Section 3 and Section 4 applies.

2 Background results

We recall some important notions and results which are necessary for this paper.

Definition 2.1 [9] *Let $\mathbb{D}$ be an integral domain and let f be a monic polynomial in $\mathbb{D}[x]$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$, counted with multiplicity. The* discriminant *of f is given by*

$$D(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

The discriminant is a symmetric function in the roots of f and thus lies in $\mathbb{D}$. A polynomial f contains multiple roots if and only if $D(f) = 0$. If $D(f) \neq 0$ then we call f *squarefree.*

Proposition 2.2 [9] *An alternate formula for the discriminant of f is*

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i).$$

Next is the result, due to Stickelberger, used in this paper which relates the parity of the number of irreducible factors of a polynomial with its discriminant.

Theorem 2.3 [12–14] *Let p be an odd prime and suppose that f is a monic polynomial of degree n with integral coefficients in a p-adic field $\mathbb{F}$. Let $\bar{f}$ be the result of reducing the coefficients of $f \pmod{p}$. Assume further that $\bar{f}$ has no repeated roots. If $\bar{f}$ has r irreducible factors over the residue class field, then $r \equiv n \pmod{2}$ if and only of $D(f)$ is a square in $\mathbb{F}$.*

The main result used in this paper is the application of the above theorem, due to Swan [14], to finite fields of odd characteristic.

Corollary 2.4 *Let q be a power of an odd prime p and let $\mathbb{F}_q$ be the finite field with q elements. Let g be a polynomial over $\mathbb{F}_q$ of degree n with no repeated roots. Furthermore, let r be the number of irreducible factors of g over $\mathbb{F}_q$. Then $r \equiv n \pmod{2}$ if and only if $D(g)$ is a square in $\mathbb{F}_q$.*

Swan extends the previous result to the case $p = 2$ by noting that a p-adic integer a coprime to p, is a p-adic square if and only if a is a square $\pmod{4p}$.

Corollary 2.5 *Let g be a polynomial of degree n over $\mathbb{F}_2$ with $D(g) \neq 0$ and let f be a monic polynomial over the 2-adic integers such that g is the reduction of $f \pmod{2}$. Furthermore, let r be the number of irreducible factors of g over $\mathbb{F}_2$. Then $r \equiv n \pmod{2}$ if and only if $D(f) \equiv 1 \pmod{8}$.*

We observe that if a polynomial has an even number of irreducible factors then it is reducible. However, if the polynomial has an odd number of irreducible factors, we cannot say more. Therefore, Swan-like results are useful in giving reducibility conditions for polynomials.

If f is a monic polynomial over $\mathbb{F}_q$ with $f(0) \neq 0$, we denote the *monic reverse* of f by $\mathrm{rev}(f)$, where, if a_0 is the constant term of f, $\mathrm{rev}(f(x)) = {a_0}^{-1} x^n f(1/x)$. It is well known that a polynomial and its reverse have the same number of irreducible factors [14]. If f defines the trinomial $f(x) = x^n + x^k + 1 \in \mathbb{F}_2[x]$, then the reverse is given by $\mathrm{rev}(f(x)) = x^n + x^{n-k} + 1$.

We now summarize Swan's Theorem characterizing the parity of the number of irreducible factors of a trinomial over $\mathbb{F}_2$.

Theorem 2.6 [14] *Let $n > k > 0$ and assume that precisely one of n, k is odd. Furthermore, let r be the number of irreducible factors of $f(x) = x^n + x^k + 1 \in \mathbb{F}_2[x]$. Then $r \equiv 0 \pmod 2$ is in the following cases:*

- *n even, k odd, $n \neq 2k$ and $nk/2 \equiv 0, 1 \pmod 4$;*
- *n odd, k even, $k \nmid 2n$ and $n \equiv 3, 5 \pmod 8$;*
- *n odd, k even, $k \mid 2n$ and $n \equiv 1, 7 \pmod 8$.*

In other cases f has an odd number of factors.

The case where n and k are both odd can be covered by making use of the fact that the reverse of f has the same number of irreducible factors. If both n and k are even the trinomial is a square and has an even number of irreducible factors.

For practical applications the following corollary is important.

Corollary 2.7 *No binary trinomial with degree a multiple of 8 is irreducible.*

To determine whether $D(f)$ is a square in a finite field we introduce the *quadratic character*.

Definition 2.8 *Let p be an odd prime and let $q = p^m, m \geq 1$. The quadratic character, η, of $\alpha \in \mathbb{F}_q^*$ is given by*

$$\eta(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is a quadratic residue in } \mathbb{F}_q; \\ -1 & \text{otherwise.} \end{cases}$$

The quadratic character is a homomorphism (and thus preserves multiplication) from $\mathbb{F}_q^*$ to the complex numbers. If q is prime, the quadratic character is equivalent to the Legendre symbol (mod q).

Gauss' lemma gives a computationally friendly method of calculating the quadratic character. Let $\alpha \in \mathbb{F}_q^*$, then $\eta(\alpha) = \alpha^{(q-1)/2}$. Of particular interest is the evaluation of the quadratic character at $\alpha = -1$. We have

$$\eta(-1) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4; \\ -1 & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

We note that $q \equiv 3 \pmod 4$ if and only if $p \equiv 3 \pmod 4$ and $m \equiv 1 \pmod 2$.

In each of the following sections we further comment on other previous works which are closely related to this paper.

3 Binomials

Irreducible binomials over finite fields have been studied in [9, 11]. In [9] a sufficient and necessary condition is given for when a binomial over $\mathbb{F}_q$ is irreducible. In [11], given a finite field of characteristic p, the authors give precisely for which degrees there exist irreducible binomials. Swan-like results can give simple conditions to determine the parity of the number of irreducible factors of a binomial over $\mathbb{F}_q$. These conditions complement the irreducibility criteria by providing an easy method of checking if a binomial over $\mathbb{F}_q$ is reducible. First, we state the previous results outlined above.

Theorem 3.1 [9, Theorem 3.75] *Let $t \geq 2$ be an integer and $a \in \mathbb{F}_q^*$. Then the binomial $x^t - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if the following two conditions hold: (i) each prime factor of t divides the order e of a in $\mathbb{F}_q^*$, but not $(q-1)/e$; (ii) $q \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$.*

We now state a theorem for a general q to determine for which degrees m there are irreducible binomials over $\mathbb{F}_q$.

Theorem 3.2 [11] *Let $\mathbb{F}_q$ be a finite field of odd characteristic p, $q \geq 5$. There exists an irreducible binomial over $\mathbb{F}_q$ of degree m, $m \not\equiv 0 \pmod 4$, if and only if every prime factor of m is also a prime factor of $q-1$. For $m \equiv 0 \pmod 4$ then there exists an irreducible binomial over $\mathbb{F}_q$ of degree m if and only if $q \equiv 1 \pmod 4$ and every prime factor of m is also a prime factor of $q-1$.*

The condition that $q \geq 5$ in the above theorem is necessary due to the small size of $\mathbb{F}_3$. Indeed, the only irreducible binomial over $\mathbb{F}_3$ is $x^2 + 1$.

These results give sufficient and necessary conditions to determine the irreducibility for binomials over $\mathbb{F}_q$. However, the application of these theorems requires knowledge of the factorization of $q-1$, which may be large. Efficient large integer factorization is a well-known hard problem, for a survey on the subject see [8].

We focus now on Swan-like results for binomials over finite fields of odd characteristic which do not require any such factorization. The results here depend on the congruences of the degree, on the characteristic (mod 4) and on the evaluation of the quadratic character. These results give the parity of the number of irreducible factors of a given binomial and thus can prove only reducibility. It is important to note, however, that the computation of the quadratic character is simple and requires computing one power, rather than integer factorization.

We present, as a lemma, the discriminant of a binomial.

Lemma 3.3 *Let $f(x) = x^n + a$. If $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are the roots of f in the splitting field of f,*

$$D(f) = (-1)^{n(n-1)/2} \prod_{i=0}^{n-1} n\alpha_i^{n-1} = (-1)^{n(n-1)/2} n^n a^{n-1}.$$

By Corollary 2.4, if r is the number of irreducible factors of f, then $n \equiv r \pmod 2$ if and only if $\eta(D(f)) = 1$.

Theorem 3.4 *Let q be a power of an odd prime p and let $f(x) = x^n + a \in \mathbb{F}_q[x]$, where $a \neq 0$ and p does not divide n. Let η be the quadratic character of $\mathbb{F}_q$ and let $D(f)$ be the discriminant of f. Then $\eta(D(f)) = 1$ if and only if one of the following cases hold:*

1. $q \equiv 1 \pmod 4$, $n \equiv 0 \pmod 2$ *and a is a quadratic residue in $\mathbb{F}_q$,*
2. $q \equiv 1 \pmod 4$, $n \equiv 1 \pmod 2$ *and n is a quadratic residue in $\mathbb{F}_q$,*
3. $q \equiv 3 \pmod 4$, $n \equiv 2 \pmod 4$ *and a is a quadratic non-residue in $\mathbb{F}_q$,*
4. $q \equiv 3 \pmod 4$, $n \equiv 3 \pmod 4$ *and n is a quadratic non-residue in $\mathbb{F}_q$,*
5. $q \equiv 3 \pmod 4$, $n \equiv 0 \pmod 4$ *and a is a quadratic residue in $\mathbb{F}_q$,*
6. $q \equiv 3 \pmod 4$, $n \equiv 1 \pmod 4$ *and n is a quadratic residue in $\mathbb{F}_q$.*

PROOF. We know that $D(f)$ is a square in $\mathbb{F}_q$ if and only if

$$\eta\left(D(f)\right) = \eta\left((-1)^{n(n-1)/2}\right)\eta\left(n^n\right)\eta\left(a^{n-1}\right) = 1. \tag{1}$$

Equation (1) holds if and only if each term in the product is 1 or if exactly two terms in the product are -1. We analyze conditions under which these cases hold.

Case 1. Two terms equal to -1

We immediately rule out the case where the final two terms in Equation (1) are equal to -1 since if $n \equiv 0 \pmod 2$ then $\eta(n^n) = \eta^n(n) = 1$, and if $n \equiv 1 \pmod 2$ then $\eta(a^{n-1}) = \eta^{n-1}(a) = 1$. Therefore the first term must equal -1, which occurs if and only if $q \equiv 3 \pmod 4$ and $n \equiv 2, 3 \pmod 4$.

Let $q \equiv 3 \pmod 4$. If $n \equiv 2 \pmod 4$ then the second term is always 1 and $\eta(D(f)) = 1$ if and only if a is a quadratic non-residue. If $n \equiv 3 \pmod 4$ then the third term is always 1 and $\eta(D(f)) = 1$ if and only if n is a quadratic non-residue.

Case 2. All terms equal to 1

We have from above that the first term of Equation (1) is 1 if and only if $q \equiv 1 \pmod 4$, or $q \equiv 3 \pmod 4$ and $n \equiv 0, 1 \pmod 4$.

Suppose $q \equiv 1 \pmod 4$. If $n \equiv 0 \pmod 2$, $\eta(n^n) = \eta^n(n) = 1$ and $\eta(D(f)) = 1$ if and only if a is a quadratic residue. If $n \equiv 1 \pmod 2$, we have $\eta(a^{n-1}) = \eta^{n-1}(a) = 1$ and so $\eta(D(f)) = 1$ if and only if n is a quadratic residue.

Now, suppose $q \equiv 3 \pmod 4$, then $n \equiv 0, 1 \pmod 4$ and the reasoning is identical to the previous case. ∎

We can infer reducibility conditions on binomials from Theorem 3.4 by observing the conditions in the statement of the theorem and the parity of

the degree n of the binomial f. Thus, f is reducible if n is even and the condition is met or if n is odd and the condition is not met. In all other cases, f has an odd number of irreducible factors and we cannot say more. Below, we give an example of these results and note that while these are conditions on reducibility (and not irreducibility, which is the usual problem), the computations are simple.

Corollary 3.5 *Let q be a power of an odd prime p and let $f(x) = x^n + a \in \mathbb{F}_q[x]$, where $a \neq 0$ and p does not divide n. Then f is reducible if $n \equiv 0 \pmod 4$ and a is a quadratic residue or if $n \equiv 1 \pmod 4$ and n is a quadratic non-residue.*

4 Trinomials

In this section we are interested in trinomials $x^n + ax^k + b$, $ab \neq 0$, over $\mathbb{F}_q$ where q is a power of an odd prime p. The parity of the number of irreducible factors of trinomials over $\mathbb{F}_q$ depends on the congruence $q \pmod 4$ and also on evaluation of the quadratic character of a, b, n and k in $\mathbb{F}_q$. We analyze some special congruences to give Swan-like results for general odd characteristic. First, we present as a lemma, the discriminant of a trinomial as given by Swan.

Lemma 4.1 [14] *Let $f(x) = x^n + ax^k + b$, with $n > k > 0$ and $ab \neq 0$. Let $d = \gcd(n, k)$ so that $k = dk_1$ and $n = dn_1$. Then*

$$D(x^n + ax^k + b) = (-1)^{\frac{n(n-1)}{2}} b^{k-1} \cdot \left[n^{n_1} b^{n_1-k_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1} k^{k_1} a^{n_1}\right]^d. \quad (2)$$

A sharp difference in analyzing the discriminant between extensions of characteristic 2, which was covered by Vishne in [15], and in the odd characteristic case covered in this paper, is in the p-adic analysis. For characteristic 2, Vishne requires evaluating the discriminant of a trinomial $(\text{mod } 8R)$ where R is a valuation ring of the 2-adic numbers. Vishne's case is a direct analogue of Swan's proof over $\mathbb{F}_2$. In our case, since p is an odd prime, we consider the discriminant as lying within the ground field.

Let p be an odd prime and let $q = p^m$, for some $m \geq 1$. We observe that the formulas for the discriminants of binomials and trinomials, given in Lemma 3.3 and Lemma 4.1 respectively, remain unchanged when f is considered as a polynomial over the extension field $\mathbb{F}_q$.

We now give conditions under which the discriminant of a trinomial is a quadratic residue in $\mathbb{F}_q$. We recall that, by Corollary 2.4, if the discriminant is a square then the degree of the trinomial and its number of irreducible factors have like parity. With the large number of cases, we do not use the notation of the quadratic character η and we simply comment on if the factors in Equation (2) are quadratic residues.

Theorem 4.2 *Let p be an odd prime and let $q = p^m$ for some $m \geq 1$. Let $f(x) = x^n + ax^k + b$, $ab \neq 0$, be a squarefree trinomial over $\mathbb{F}_q$ and let $d = \gcd(n, k)$. We proceed in cases by analyzing congruences in Equation (2).*

Case 1: $d = \gcd(n, k) \equiv 0 \pmod 2$

$D(f)$ *is a square if and only if*

1. $q \equiv 1 \pmod 4$ *and* b *is a quadratic residue in* $\mathbb{F}_q$*;*
2. $q \equiv 3 \pmod 4$, $n \equiv 0 \pmod 4$ *and* b *is a quadratic residue in* $\mathbb{F}_q$*;*
3. $q \equiv 3 \pmod 4$, $n \equiv 2 \pmod 4$ *and* b *is a quadratic non-residue in* $\mathbb{F}_q$*.*

Case 2: $d \equiv 1 \pmod 2$ *and* p *divides* n

$D(f)$ *is a square if and only if*

1. $n \equiv 0 \pmod 2$
   (a) $q \equiv 1 \pmod 4$*;*
   (b) $q \equiv 3 \pmod 4$ *and* $n \equiv 0 \pmod 4$*;*
2. $n \equiv k \equiv 1 \pmod 2$
   (a) $q \equiv 1 \pmod 4$, a *and* k *are both quadratic residues or non-residues in* $\mathbb{F}_q$*;*
   (b) $q \equiv 3 \pmod 4$, $n \equiv 1 \pmod 4$ *and* a *and* k *are both quadratic residues or non-residues in* $\mathbb{F}_q$*;*
   (c) $q \equiv 3 \pmod 4$, $n \equiv 3 \pmod 4$ *and exactly one of* a *and* k *is a quadratic residue in* $\mathbb{F}_q$*;*
3. $n \equiv 1 \pmod 2, k \equiv 0 \pmod 2$
   (a) $q \equiv 1 \pmod 4$*, exactly two of* a, b, k *are quadratic residues in* $\mathbb{F}_q$ *or none of* a, b, k *are quadratic residues in* $\mathbb{F}_q$*;*
   (b) $q \equiv 3 \pmod 4$, $n \equiv 3 \pmod 4$ *and exactly one of* a, b, k *are quadratic residues in* $\mathbb{F}_q$ *or all of* a, b, k *are quadratic residues in* $\mathbb{F}_q$*;*
   (c) $q \equiv 3 \pmod 4$, $n \equiv 1 \pmod 4$ *and none of* a, b, k *are quadratic residues in* $\mathbb{F}_q$ *or exactly two of* a, b, k *are quadratic residues in* $\mathbb{F}_q$*.*

Case 3: $d \equiv 1 \pmod 2$ *and* p *divides* k*, or* p *divides* $n - k$

$D(f)$ *is a square if and only if*

1. $q \equiv 1 \pmod 4, n \equiv 0 \pmod 2$ *and* b *is a quadratic residue in* $\mathbb{F}_q$*, or* $q \equiv 3 \pmod 4, n \equiv 0 \pmod 2$ *and* b *is a quadratic non-residue in* $\mathbb{F}_q$*;*
2. $q \equiv 1 \pmod 4, n \equiv 1 \pmod 2$ *and* n *is a quadratic residue in* $\mathbb{F}_q$*, or* $q \equiv 3 \pmod 4, n \equiv 1 \pmod 2$ *and* n *is a quadratic non-residue in* $\mathbb{F}_q$*.*

Proof. We proceed by cases.

Case 1: $d \equiv 0 \pmod 2$

The last term in Equation (2) is a square and so $D(f)$ a square if and only if $(-1)^{\frac{n(n-1)}{2}} b^{k-1}$ is a square. Since $d = \gcd(n, k)$ is even, so are n and k and we have the following cases.

1.1 If $q \equiv 1 \pmod 4$, then -1 is a quadratic residue. Since k is even, b^{k-1} is a square if and only if b is a quadratic residue.
1.2 If $q \equiv 3 \pmod 4$ and $n \equiv 0 \pmod 4$, then $(-1)^{\frac{n(n-1)}{2}} = 1$ and the analysis is the same as in Case 1.1.
1.3 If $q \equiv 3 \pmod 4$ and $n \equiv 2 \pmod 4$, then $(-1)^{\frac{n(n-1)}{2}} = -1$ which is a quadratic non-residue. The remainder of the analysis is similar to Case 1.1.

If d is odd, we can assume $d = 1$ by factoring the remaining $d - 1$ power, which is a square. We then have the following cases.

Case 2: $d \equiv 1 \pmod 2$ *and* p *divides* n

If p divides n then the last term in Equation (2) is $(-1)^{2n_1-k_1+1} k^{n_1-k_1} k^{k_1} a^{n_1}$. Thus

$$D(f) \equiv (-1)^{2n_1-k_1+1+\frac{n(n-1)}{2}} b^{k-1} (ak)^{n_1} \pmod p.$$

We proceed by cases:

2.1 If n is even (hence k and k_1 are odd, and n_1 is even), $D(f)$ is a square if and only if $(-1)^{\frac{n(n-1)}{2}}$ is a square. This occurs if and only if $q \equiv 1 \pmod 4$, or $q \equiv 3 \pmod 4$ and $n \equiv 0 \pmod 4$.
2.2 If n is odd and k is odd (hence so are n_1 and k_1), $D(f)$ is a square if and only if $(-1)^{\frac{n(n-1)}{2}} ak$ is a square. The analysis is as before.
2.3 If n is odd and k is even (hence n_1 is odd and k_1 is even), $D(f)$ is a square if and only if $(-1)^{\frac{n(n-1)}{2}+1} abk$ is a square. The analysis is as before.

Case 3: $d \equiv 1 \pmod 2$ *and* p *divides* k *or* p *divides* $n - k$

If p divides k then $D(f) \equiv (-1)^{\frac{n(n-1)}{2}} b^{k-k_1+n_1-1} n^{n_1} \pmod p$. Since k and k_1 have like parity, we have:

3.1 If n is even (hence n_1 is even), $D(f)$ is a square if and only if $(-1)^{\frac{n(n-1)}{2}} b$ is a square.
3.2 If n is odd (hence n_1 is odd), $D(f)$ is a square if and only if $(-1)^{\frac{n(n-1)}{2}} n$ is a square.

An analysis similar to that found in Case 2 concludes this theorem. ■

Remark *There are several trinomials over* $\mathbb{F}_q$ *not covered by Theorem 4.2. Since each of* a *and* b *vary over* $\mathbb{F}_q^*$ *and we need to consider the congruences* $q \pmod 4$ *and the reductions of* n *and* $k \pmod p$*, the total number of cases*

is $2p^2(q-1)^2$. *Some of these cases are simple; for example, since* f *and its reverse have the same number of irreducible factors, we need only consider half of these trinomials. Furthermore, by Theorem 4.2, we determine the parity of the number of irreducible factors of the trinomial if* n *and* k *are both even, or if* p *divides* n, k *or* $n-k$. *Since the* p *dividing* $n-k$ *case is not independent of the congruences of* n *and* $k \pmod p$, *we reduce the total number of cases on congruences of* n, k *and* $n-k$ *by between* $2p$ *and* $3p$. *Thus, the total number of remaining cases lies (strictly) between* $3(p^2-3p)(q-1)^2/4$ *and* $3(p^2-2p)(q-1)^2/4$. *If Rem(p) is the proportion of remaining cases, we have*

$$\frac{3(p^2-3p)(q-1)^2/4}{2p(q-1)^2} = \frac{3}{8}\left(1-\frac{3}{p}\right) < Rem(p) < \frac{3}{8}\left(1-\frac{2}{p}\right).$$

Theorem 4.2 covers a large proportion of the total number of trinomials when p *is small. For example, when* $p = 3$ *an upper bound on the proportion of remaining cases is* $1/8 = 12.5\%$ *and if* $p = 5$ *this bound is* $9/40 = 22.5\%$. *When* p *becomes large, the bounds on the proportion of cases not covered by Theorem 4.2 converge to* $3/8 = 37.5\%$.

In the remaining cases, Theorem 4.2 does not apply if p *does not divide* n, k *or* $n-k$. *For example, we cannot conclude anything from Theorem 4.2 about trinomials* $x^{4m+1} + x^2 + 4 \in \mathbb{F}_5[x]$ *when* 5 *does not divide* $4m+1$ *or* $4m-1$ *(that is, when* $m \not\equiv \pm 1 \pmod 5$*). However, it is easy to check that trinomials of this form have* 2 *as a root.*

In the cases not covered, the confounding term is in the second line of Equation (2):

$$n^{n_1} b^{n_1-k_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1} k^{k_1} a^{n_1}.$$

In particular, computing the discriminant in these cases relies on computing the quadratic character in $\mathbb{F}_q$. *Given* q, *this calculation can easily be done by computer; however as far as we know, general results on additive properties of the quadratic character are unknown and likely hard.*

As an example, we consider trinomials of the form $x^{mp}-x-a \in \mathbb{F}_q[x], a \neq 0$. The special case of these trinomials when q is prime and $m = 1$ was studied by Serret, see [9]. Serret proves a strong result that polynomials of this form are irreducible over $\mathbb{F}_p$. We consider the parity of the number of irreducible factors of trinomials of the more general form $x^{mp} - x - a \in \mathbb{F}_q[x]$, where m is a positive integer.

Corollary 4.3 *Let* $f(x) = x^{mp} - x - a \in \mathbb{F}_q[x]$, $a \neq 0$. *Then* f *has an odd number of irreducible factors if and only if* $m \equiv 1 \pmod 4$, $m \equiv 3 \pmod 4$ *and* $q \equiv 1 \pmod 4$, *or* $m \equiv 2 \pmod 4$ *and* $q \equiv 3 \pmod 4$.

Proof. We break into cases based on the congruence of $m \pmod 4$. For each value of $m \pmod 4$, we cite the cases that we apply from Theorem 4.2.

If $m \equiv 1 \pmod 4$, $D(f)$ satisfies one of Case 2.2a or 2.2c which shows that $f(x)$ always has an odd number of irreducible factors.

If $m \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$, then $D(f)$ satisfies Case 2.2a and f has an odd number of irreducible factors. If $m \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$, then $D(f)$ fails to satisfy Case 2.2b and f has an even number of irreducible factors.

If $m \equiv 0 \pmod 4$ then $D(f)$ satisfies either Case 2.1a or Case 2.1b and thus f has an even number of irreducible factors for all q.

Suppose $m \equiv 2 \pmod 4$. For $q \equiv 1 \pmod 4$, $D(f)$ satisfies Case 2.1a and thus f has an even number of irreducible factors. For $q \equiv 3 \pmod 4$, $D(f)$ fails to satisfy Case 2.1b and thus f has an odd number of irreducible factors. ∎

5 Extensions

We now present some examples of polynomials for which we can apply the methods used in this paper to comment on the parity of the number of irreducible factors in each case. We note that when this work was well advanced, we found that the subsequent examples were special cases of the article by Kim and Koepf [6]. We leave these results here as further examples of Swan-like results using the same method we used for the binomial and trinomial cases; more information about these examples can be found in [6].

5.1 Affine polynomials over $\mathbb{F}_q$, q odd

Let p be an odd prime and let $q = p^s$, with $s \geq 1$. A *linearized polynomial* over $\mathbb{F}_q$ is a polynomial of the form $L(x) = \sum_{i=0}^{n} c_i x^{q^i}$. An *affine polynomial over* $\mathbb{F}_{q^m}$ is a polynomial of the form $L(x) - \alpha$ where $L(x)$ is a linearized polynomial in $\mathbb{F}_q[x]$ and $\alpha \in \mathbb{F}_{q^m}$.

Let $A(x)$ be an affine polynomial over $\mathbb{F}_{q^m}$. Thus, $A(x) = \alpha + a_1 x^{q^{i_1}} + a_2 x^{q^{i_2}} + \cdots + a_n x^{q^{i_n}}$ where $\alpha \in \mathbb{F}_{q^m}$, $a_1, a_2, \ldots, a_n \in \mathbb{F}_q^*$ and $0 \leq i_1 < i_2 < \cdots < i_n$. We compute the discriminant of $A(x)$ using the form

$$D(A) = (-1)^{\frac{q^{i_n}(q^{i_n}-1)}{2}} \prod_{i=1}^{q^{i_n}} A'(\alpha_i),$$

where $\alpha_1, \ldots, \alpha_{q^{i_n}}$ are the roots of A in an extension of $\mathbb{F}_q$. We observe that if $i_1 \neq 0$ then it is clear that A is a qth power and thus $D(A) = 0$. Now, we suppose $i_1 = 0$.

Theorem 5.1 *Let p be an odd prime and let $q = p^m$, for some $m \geq 1$. Also, let $A(x) = \alpha + a_1 x + a_2 x^{q^{i_2}} + \cdots + a_n x^{q^{i_n}}$ be an affine polynomial over $\mathbb{F}_{q^m}$. Then $A(x)$ has an odd number of irreducible factors if and only if*

1. *$q \equiv 1 \pmod 4$ and a_1 is a quadratic residue in $\mathbb{F}_q$,*
2. *$q \equiv 3 \pmod 4$, $i_n \equiv 0 \pmod 2$ and a_1 is a quadratic residue in $\mathbb{F}_q$,*

3. $q \equiv 3 \pmod 4$, $i_n \equiv 1 \pmod 2$ *and* a_1 *is a quadratic non-residue in* $\mathbb{F}_q$.

PROOF. Let $A(x)$ be as in the hypothesis. Then $D(A) = (-1)^{q^{i_n}(q^{i_n}-1)/2} a_1$. Thus $D(A)$ is a square in $\mathbb{F}_q$ if and only if either both terms are quadratic residues or both terms are quadratic non-residues in $\mathbb{F}_q$.

If $q \equiv 1 \pmod 4$ then $D(A)$ is a square in $\mathbb{F}_q$ if and only if a_1 is a quadratic residue in $\mathbb{F}_q$.

If $q \equiv 3 \pmod 4$ then $(-1)^{q^{i_n}(q^{i_n}-1)/2} = 1$ if and only if i_n is even. Thus, $D(A)$ is a square in $\mathbb{F}_q$ if and only if i_n is even and a_1 is a quadratic residue or if i_n is odd and a_1 is a quadratic non-residue in $\mathbb{F}_q$. ∎

5.2 Composition with linearized polynomials

Let $L(x) = \sum_{i=0}^{n} c_i x^{q^i}$ be a linearized polynomial over $\mathbb{F}_q$ and let $f = g \circ L$ for some $g \in \mathbb{F}_q[x]$, with $\deg(g) > 1$. The discriminant of f is given by

$$\begin{aligned} D(f) &= (-1)^{T(T-1)/2} \prod_{i=1}^{T} f'(\alpha_i) \\ &= (-1)^{T(T-1)/2} \prod_{i=1}^{T} g'(L(\alpha_i)) L'(\alpha_i), \end{aligned}$$

where $T = q^n \cdot \deg(g)$ and the α_i are the roots of f in an extension of $\mathbb{F}_q$. If $c_0 = 0$, then $D(f) = 0$ and thus f has repeated roots.

If $c_0 \neq 0$ then 0 is a root of f with multiplicity 1. Thus

$$D(f) = g'(c_0) c_0^T \prod_{\alpha_i \neq 0} g'\left(L(\alpha_i)\right) \in \mathbb{F}_q.$$

Since $g'(c_0), c_0 \in \mathbb{F}_q$, thus so is $\prod_{\alpha_i \neq 0} g'\left(L(\alpha_i)\right)$.

Determining the parity of the number of irreducible factors r of f depends on the polynomials g and L. In particular, we conclude that $r \equiv T \pmod 2$ if and only if each of $g'(c_0), c_0^T$ and $\prod_{\alpha_i \neq 0} g'\left(L(\alpha_i)\right)$ are all quadratic residues in $\mathbb{F}_q$ or if exactly one of them is.

References

1. O. Ahmadi, On the distribution of irreducible trinomials over $\mathbb{F}_3$, *Finite Fields and Their Applications*, **13** (2007), 659-664.
2. A. Bluher, A Swan-like theorem, *Finite Fields and Their Applications*, **12** (2006), 128-138.
3. R. Brent and P. Zimmerman, Ten new primitive binary trinomials, *Mathematics of Computation*, **78** (2009), 1197-1199.

4. J. von zur Gathen, Irreducible trinomials over finite fields, *Mathematics of Computation*, **72** (2003), 1987-2000.
5. A. Hales and D. Newhart, Swan's theorem for binary tetranomials, *Finite Fields and Their Applications*, **12** (2006), 301-311.
6. R. Kim and W. Koepf, Parity of the number of irreducible factors for composite polynomials, *Finite Fields and Their Applications*, **16** (2010), 137-143.
7. W. Koepf and R. Kim, The parity of the number of irreducible factors for some pentanomials, *Finite Fields and Their Applications*, **15** (2009), 585-603.
8. A. Lenstra, Integer factoring, *Designs, Codes and Cryptography*, **19** (2000), 101-128.
9. R. Lidl and H. Neiderreiter, *Finite Fields*, Cambridge University Press, UK, (1997).
10. P. Loidreau, On the factorization of trinomials over $\mathbb{F}_3$, INRIA rapport de recherche, no.: 3918 (2000).
11. D. Panario and D. Thomson, Efficient pth root computation in finite fields of characteristic p, *Designs, Codes and Cryptography*, **50** (2009), 351-358.
12. A. Pellet, Sur la décomposition d'une fonction entière en facteurs irréductibles suivant un module premier p, *Comptes Rendus de l'Académie des Sciences Paris*, **86** (1878), 1071-1072.
13. L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, *Verhandlungen des ersten Internationalen Mathematiker-Kongresses*, Zürich (1897), 182-193.
14. R. Swan, Factorization of polynomials over finite fields, *Pacific Journal of Mathematics*, **12** (1962), 1099-1106.
15. U. Vishne, Factorization of trinomials over Galois fields of characteristic 2, *Finite Fields and their Applications*, **3** (1997), 370-377.
16. Z. Zhao and X. Cao, A note on the reducibility of binary affine polynomials, *Designs, Codes and Cryptography*, **57** (2010), 83-90.