A NOTE ON THE ROOTS OF TRINOMIALS OVER A FINITE FIELD

ROBERT COULTER AND MARIE HENDERSON*

ABSTRACT. For non-negative integers \( n \) we determine the roots of the trinomial \( X^{p^n} - aX - b \), with \( a \neq 0 \), over a finite field of characteristic \( p \).

Throughout \( q = p^k \) where \( p \) is a prime and \( k \) is a positive integer. Let \( \mathbb{F}_q \) be the finite field of order \( q \), \( \mathbb{F}_q^* \) be the set of non-zero elements of \( \mathbb{F}_q \) and \( \mathbb{F}_q[X] \) be the ring of polynomials in the indeterminate \( X \) over \( \mathbb{F}_q \). In this article we determine the roots of the trinomial \( f \in \mathbb{F}_q[X] \) given by

\[
f(X) = X^{p^n} - aX - b
\]

(1)

where \( n \) is a positive integer. Throughout we assume \( a \in \mathbb{F}_q^* \) as otherwise \( f \) is a binomial and the factorisation is known, see [3]. The trinomial (1) has been considered in [2] for the case \( a = 1 \). The article [4] mainly considers the case where \( n \) divides \( k \). There is one result in [4] concerning the general case which we include below (see Lemma 2). We determine all roots of the trinomial (1) in Theorem 3 below and then cast these against the previous results described above.

We make use of the following lemma. This is essentially [1, Theorem 57].

**Lemma 1.** For positive integers \( r \) and \( k = md \) define

\[
I_r = \{ ir \mod k | 0 \leq i \leq m - 1 \}.
\]

If \( n \) is a positive integer satisfying \( \gcd(n, k) = d \), then \( I_n = I_d \).

The following lemma appears as Theorem 2 of [4].

**Lemma 2.** Let \( q = p^k \), \( n \) be a positive integer and \( f(X) = X^{p^n} - aX - b \) where \( a \in \mathbb{F}_q^* \) and \( b \in \mathbb{F}_q \). Then, in the field \( \mathbb{F}_q \), \( f \) has either zero, one or \( p^d \) roots where \( d = \gcd(n, k) \).

1991 Mathematics Subject Classification. 11T06.

*This author performed some of this work while at RMIT University and was supported by a RMIT VRII grant.
Following the statement of Theorem 2 in [4] the author remarks that it seems difficult to characterise the roots of (1). The following theorem gives the full solution to this problem.

**Theorem 3.** Let \( q = p^k \), \( n \) be a non-negative integer and \( f \in \mathbb{F}_q[X] \) be the trinomial \( f(X) = X^{p^n} - aX - b \) where \( a \in \mathbb{F}_q^* \). Set \( d = \gcd(n, k) \) and \( m = k/d \). Let \( \text{Tr}_d \) be the trace function from \( \mathbb{F}_q \) onto \( \mathbb{F}_{p^d} \). For \( 0 \leq i \leq m - 1 \), define \( t_i = \sum_{j=1}^{m-2} p^{n(j+1)} \). Put \( \alpha_0 = a \) and \( \beta_0 = b \). If \( m > 1 \), then for \( 1 \leq r \leq m-1 \), set \( \alpha_r = a^{1+p^n+\dotsc+p^{nr}} \) and

\[
\beta_r = \sum_{i=0}^{r} \alpha^i b^{p^{ni}}
\]

where \( s_i = \sum_{j=1}^{r-1} p^{n(j+1)} \) for \( 0 \leq i \leq r - 1 \) and \( s_r = 0 \). The trinomial \( f \) has no roots in \( \mathbb{F}_q \) if and only if \( \alpha_{m-1} = 1 \) and \( \beta_{m-1} \neq 0 \). When \( \alpha_{m-1} \neq 1 \) then \( f \) has a unique root \( x \in \mathbb{F}_q \), namely, \( x = \beta_{m-1}/(1 - \alpha_{m-1}) \). Otherwise \( f \) has \( p^d \) roots in \( \mathbb{F}_q \) given by \( x + \delta \tau \) where \( \delta \in \mathbb{F}_{p^d} \), \( \tau \) is a fixed element of \( \mathbb{F}_q \) satisfying \( \tau^{p^n-1} = a \) and, for any \( c \in \mathbb{F}_q^* \) satisfying \( \text{Tr}_d(c) \in \mathbb{F}_{p^d} \),

\[
x = \frac{1}{\text{Tr}_d(c)} \sum_{i=0}^{m-1} \left( \sum_{j=0}^{i} c^{p^{nj}} \right) a^i b^{p^{ni}}.
\]

**Proof.** For any \( y \in \mathbb{F}_q \) we have \( y^{p^n} = y^{p^{(n/d)}} = y \). It follows that \( \alpha_{m-1}^{p^n} = \alpha_{m-1} \) and \( \beta_{m-1}^{p^n} = a \beta_{m-1} - b \alpha_{m-1} + b \). For \( 0 \leq r \leq m-2 \), similar calculations give \( \alpha_r^{p^n} = a^{-1} \alpha_{r+1} \) and \( \beta_r^{p^n} = a^{\beta^{p^n(r+1)}} \beta_r - a^{-1} b \alpha_{r+1} + b \).

Suppose we have \( y^{p^n} = ay + b \) for some \( y \in \mathbb{F}_q \). Given an integer \( i \), \( 1 \leq i \leq m - 1 \), for which \( y^{pni} = a y_i + \beta_{i-1} \) then

\[
y^{pni+1} = \alpha_i y^{pni} + \beta_{i-1}^{p^n} = \alpha_i y + b + \beta_{i-1}^{p^n} = \alpha_i y + a^{-1} b \alpha_i + a^{\beta^{p^n} \beta_{i-1} - a^{-1} b \alpha_i + b^{pni}} = \alpha_i y + \beta_i.
\]

where we have used the identity \( \beta_r = a^{\beta^{p^n} \beta_{r-1} + b^{p^{nr}}} \), for \( 1 \leq r \leq m - 1 \).

As \( y^{p^n} = a y + \beta_0 \), it follows that \( y^{pni} = a y_i + \beta_{i-1} \) for all positive integers \( i \leq m \). In particular, \( y^{pnm} = a y_m + \beta_{m-1} \). Since \( y^{pnm} = y \), then \( (\alpha_{m-1} - 1)y + \beta_{m-1} = 0 \). Immediately it is seen that no root exists when \( \alpha_{m-1} = 1 \) and \( \beta_{m-1} \neq 0 \). Also, if \( \alpha_{m-1} \neq 1 \), then there exists a unique root \( y = \beta_{m-1}/(1 - \alpha_{m-1}) \).
It remains to deal with the case when \( \alpha_{m-1} = 1 \) and \( \beta_{m-1} = 0 \). Firstly, let \( c \in \mathbb{F}_q \) satisfy \( \text{Tr}_d(c) \neq 0 \). Put \( \gamma_i = \sum_{j=0}^i \epsilon^{p^{nj}} \) for \( 0 \leq i \leq m-1 \) and
\[
x = \frac{1}{\text{Tr}_d(c)} \sum_{i=0}^{m-1} \gamma_i a^{t_i} b^{p^{ni}}.
\]
Then
\[
x^{p^n} = \frac{1}{\text{Tr}_d(c)} \sum_{i=0}^{m-1} \gamma_i^{p^n} (a^{t_i})^{p^n} b^{p^{n(i+1)}}.
\]
For \( 0 \leq i \leq m-2 \) we have
\[
(a^{t_i})^{p^n} = (a^{p^{n+1}} + \ldots + p^{n(m-1)})^{p^n} = a^{t_{i+1}}.
\]
For \( i = m-1 \), \( (a^{s_m-1})^{p^n} = 1 \). We thus have
\[
x^{p^n} = \frac{\gamma_{m-1}}{\text{Tr}_d(c)} b^{p^{nm}} + \frac{a}{\text{Tr}_d(c)} \sum_{i=0}^{m-1} \gamma_i^{p^n} a^{t_{i+1}} b^{p^{n(i+1)}}
\]
\[
= b + \frac{a}{\text{Tr}_d(c)} \sum_{i=1}^{m-1} \gamma_i^{p^n} a^{t_i} b^{p^{ni}}
\]
as \( \gamma_{m-1} = \text{Tr}_d(c) \) from Lemma 1. We proceed with the calculation of \( x^{p^n} - ax \):
\[
x^{p^n} - ax = b + \frac{a}{\text{Tr}_d(c)} \sum_{i=1}^{m-1} \gamma_i^{p^n} a^{t_i} b^{p^{ni}} - \frac{a}{\text{Tr}_d(c)} \sum_{i=0}^{m-1} \gamma_i^{p^n} a^{t_i} b^{p^{ni}}
\]
\[
= b + \frac{a}{\text{Tr}_d(c)} \sum_{i=1}^{m-1} (\gamma_{i-1} - \gamma_i) a^{t_i} b^{p^{ni}} - \frac{a\gamma_0}{\text{Tr}_d(c)} a^{t_0} b.
\]
Now \( \gamma_0 = c \) and for \( 1 \leq i \leq m-1 \) we have
\[
\gamma_{i-1} - \gamma_i = \sum_{j=0}^{i-1} \epsilon^{p^{nj+1}} - \sum_{j=0}^{i} \epsilon^{p^{nj}} = \sum_{j=1}^{i} \epsilon^{p^{nj}} - \sum_{j=0}^{i} \epsilon^{p^{nj}} = -c.
\]
Therefore
\[
x^{p^n} - ax = b - \frac{ac}{\text{Tr}_d(c)} \sum_{i=0}^{m-1} a^{t_i} b^{p^{ni}} = b - \frac{ac}{\text{Tr}_d(c)} \beta_{m-1}
\]
and as \( \beta_{m-1} = 0 \) we have \( x \) is a root of \( f \).

From Lemma 1, \( \alpha_{m-1} = N_q(a) = 1 \) where \( N_q \) is the norm function from \( \mathbb{F}_{p^k} \) onto \( \mathbb{F}_{p^d} \). From [3], \( N_q(a) = 1 \) if and only if \( a = \kappa^{p^{d-1}} \) for some \( \kappa \in \mathbb{F}_q^* \). Since \( \gcd(p^n - 1, q - 1) = p^d - 1 \), then \( p^n - 1 = (p^d - 1)t \) where \( (t, q - 1) = 1 \). In other words, there exists a \( \tau \in \mathbb{F}_q^* \) satisfying \( \tau^{p^n - 1} = \kappa^{p^{d-1}} = a \). It follows that \( x + \delta \tau \) is a root of \( f \) for each \( \delta \in \mathbb{F}_{p^d} \).
From Lemma 2 there are at most $p^d$ roots of $f$ so we have obtained them all. \hfill \Box

In [2] the trinomial $g(X) = X^{p^n} - X - b$, where $b \in \mathbb{F}_q^*$, is considered. It is shown that $g$ has no roots when $\text{Tr}_d(b) \neq 0$ and $p^d$ roots when $\text{Tr}_d(b) = 0$. The final theorem of [2] aims to give a root of $g$ when $k/d$ is odd but the root given is instead a root of the polynomial $h(X) = X^{p^n} + X - b$ (in addition to this error, there is also a misprint in the statement of the theorem). We note that the proof given in [2] makes implicit use of Lemma 1. The root given in [2] can be shown to agree with that given by Theorem 3 by a direct calculation. The root constructed above when $\alpha_{m-1} \neq 1$ coincides with [4, Theorem 1] for the case $n$ divides $k$.

The following corollary is easily obtained from Theorem 3.

**Corollary 4.** Let $q = p^k$, $n$ be a positive integer and $f(X) = X^{p^n} - aX - b$ where $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. Set $l = \text{lcm}(k, n)$. The splitting field of $f$ is $\mathbb{F}_{p^l}$, where $l^t$ is the smallest integer for which $\alpha_{(lt/n)-1} = 1$ and $\beta_{(lt/n)-1} = 0$.

**References**


**Department of Mathematical Sciences, University of Delaware, Newark, Delaware 19716, U.S.A.**

*E-mail address: coulter@math.udel.edu*

*E-mail address: marie@math.udel.edu*