BULL. AUSTRAL. MATH. SOC. 11T06
VOL. 69 (2004) [429–432]

A NOTE ON THE ROOTS OF TRINOMIALS OVER A FINITE FIELD

ROBERT COULTER AND MARIE HENDERSON

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

$$f(X) = X^{p^n} - aX - b \tag{1}$$

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*

$$I_r = \{ir \bmod k \mid 0 \leqslant i \leqslant m-1\}.$$

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 $d = \gcd(n,k)$.*

Following the statement of [**4**, Theorem 2] the author remarks that it seems difficult to characterise the roots of (1). The following theorem gives the full solution to this problem.

Received 6th November, 2003
The second author performed some of this work while at RMIT University and was supported by a RMIT VRII grant.

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9727/04 $A2.00+0.00.

https://doi.org/10.1017/S0004972700036200 Published online by Cambridge University Press

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 Tr_d be the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_{p^d}$. For $0 \leqslant i \leqslant m-1$, define $t_i = \sum_{j=i}^{m-2} p^{n(j+1)}$. Put $\alpha_0 = a$ and $\beta_0 = b$. If $m > 1$, then for $1 \leqslant r \leqslant m-1$, set $\alpha_r = a^{1+p^n+\cdots+p^{nr}}$ and*

$$\beta_r = \sum_{i=0}^{r} a^{s_i} b^{p^{ni}}$$

where $s_i = \sum_{j=i}^{r-1} p^{n(j+1)}$ for $0 \leqslant i \leqslant r-1$ 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 $\delta \in \mathbb{F}_{p^d}$, τ is a fixed element of $\mathbb{F}_q$ satisfying $\tau^{p^n-1} = a$ and, for any $c \in \mathbb{F}_q^*$ satisfying $\mathrm{Tr}_d(c) \in \mathbb{F}_{p^d}^*$,

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

Proof: For any $y \in \mathbb{F}_q$ we have $y^{p^{nm}} = y^{p^{k(n/d)}} = y$. 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 $0 \leqslant r \leqslant m-2$, similar calculations give $\alpha_r^{p^n} = a^{-1}\alpha_{r+1}$ and $\beta_r^{p^n} = a^{p^{n(r+1)}}\beta_r - a^{-1}b\alpha_{r+1} + b^{p^{n(r+1)}}$.

Suppose we have $y^{p^n} = ay + b$ for some $y \in \mathbb{F}_q$. Given an integer i, $1 \leqslant i \leqslant m-1$, for which $y^{p^{ni}} = \alpha_{i-1}y + \beta_{i-1}$ then

$$\begin{aligned} y^{p^{n(i+1)}} &= \alpha_{i-1}^{p^n} y^{p^n} + \beta_{i-1}^{p^n} \\ &= \alpha_{i-1}^{p^n}(ay+b) + \beta_{i-1}^{p^n} + b \\ &= \alpha_i y + a^{-1}b\alpha_i + a^{p^{ni}}\beta_{i-1} - a^{-1}b\alpha_i + b^{p^{ni}} \\ &= \alpha_i y + \beta_i. \end{aligned}$$

where we have used the identity $\beta_r = a^{p^{nr}}\beta_{r-1} + b^{p^{nr}}$, for $1 \leqslant r \leqslant m-1$.

As $y^{p^n} = \alpha_0 y + \beta_0$, it follows that $y^{p^{ni}} = \alpha_{i-1}y + \beta_{i-1}$ for all positive integers $i \leqslant m$. In particular, $y^{p^{nm}} = \alpha_{m-1}y + \beta_{m-1}$. Since $y^{p^{nm}} = y$, 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 $\mathrm{Tr}_d(c) \neq 0$. Put $\gamma_i = \sum_{j=0}^{i} c^{p^{nj}}$ for $0 \leqslant i \leqslant m-1$ and

$$x = \frac{1}{\mathrm{Tr}_d(c)} \sum_{i=0}^{m-1} \gamma_i a^{t_i} b^{p^{ni}}.$$

https://doi.org/10.1017/S0004972700036200 Published online by Cambridge University Press

Then

$$x^{p^n} = \frac{1}{\mathrm{Tr}_d(c)} \sum_{i=0}^{m-1} \gamma_i^{p^n} (a^{t_i})^{p^n} b^{p^{n(i+1)}}.$$

For $0 \leqslant i \leqslant m-2$ we have

$$(a^{t_i})^{p^n} = (a^{p^{n(i+1)}+\cdots+p^{n(m-1)}})^{p^n} = a^{t_{i+1}} a.$$

For $i = m-1$, $(a^{s_{m-1}})^{p^n} = 1$. We thus have

$$\begin{aligned} x^{p^n} &= \frac{\gamma_{m-1}}{\mathrm{Tr}_d(c)} b^{p^{nm}} + \frac{a}{\mathrm{Tr}_d(c)} \sum_{i=0}^{m-2} \gamma_i^{p^n} a^{t_{i+1}} b^{p^{n(i+1)}} \\ &= b + \frac{a}{\mathrm{Tr}_d(c)} \sum_{i=1}^{m-1} \gamma_{i-1}^{p^n} a^{t_i} b^{p^{ni}} \end{aligned}$$

as $\gamma_{m-1} = \mathrm{Tr}_d(c)$ from Lemma 1. We proceed with the calculation of $x^{p^n} - ax$:

$$\begin{aligned} x^{p^n} - ax &= b + \frac{a}{\mathrm{Tr}_d(c)} \sum_{i=1}^{m-1} \gamma_{i-1}^{p^n} a^{t_i} b^{p^{ni}} - \frac{a}{\mathrm{Tr}_d(c)} \sum_{i=0}^{m-1} \gamma_i a^{t_i} b^{p^{ni}} \\ &= b + \frac{a}{\mathrm{Tr}_d(c)} \sum_{i=1}^{m-1} (\gamma_{i-1}^{p^n} - \gamma_i) a^{t_i} b^{p^{ni}} - \frac{a\gamma_0}{\mathrm{Tr}_d(c)} a^{t_0} b. \end{aligned}$$

Now $\gamma_0 = c$ and for $1 \leqslant i \leqslant m-1$ we have

$$\gamma_{i-1}^{p^n} - \gamma_i = \sum_{j=0}^{i-1} c^{p^{n(j+1)}} - \sum_{j=0}^{i} c^{p^{nj}} = \sum_{j=1}^{i} c^{p^{nj}} - \sum_{j=0}^{i} c^{p^{nj}} = -c.$$

Therefore

$$x^{p^n} - ax = b - \frac{ac}{\mathrm{Tr}_d(c)} \sum_{i=0}^{m-1} a^{t_i} b^{p^{ni}} = b - \frac{ac}{\mathrm{Tr}_d(c)} \beta_{m-1}$$

and as $\beta_{m-1} = 0$ we have x is a root of f.

From Lemma 1, $\alpha_{m-1} = N_d(a) = 1$ where N_d is the norm function from $\mathbb{F}_{p^k}$ onto $\mathbb{F}_{p^d}$. From [**3**], $N_d(a) = 1$ 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 exits 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 $\delta \in \mathbb{F}_{p^d}$ (giving us p^d roots). From Lemma 2 there are at most p^d roots of f so we have obtained them all. ∎

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 $\mathrm{Tr}_d(b) \neq 0$ and p^d roots when $\mathrm{Tr}_d(b) = 0$. 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

https://doi.org/10.1017/S0004972700036200 Published online by Cambridge University Press

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 $l = lcm(k, n)$. The splitting field of f is $\mathbb{F}_{p^{lt}}$, where lt is the smallest integer for which $\alpha_{(lt/n)-1} = 1$ and $\beta_{(lt/n)-1} = 0$.*

References

[1] G.H. Hardy and E.M. Wright, *An Introduction to the theory of numbers*, (fifth edition) (Oxford University Press, Oxford, 1979).

[2] J. Liang, 'On the solutions of trinomial equations over finite fields', *Bull. Calcutta Math. Soc.* **70** (1978), 379–382.

[3] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl. **20** (Addison-Wesley, Reading, 1983), (now distributed by Cambridge University Press).

[4] K. Vilanova, 'Certain trinomial equations over finite fields', *Trudy Univ. Družby Narod.* **21** (1967), 17–31.

Department of Mathematical Sciences
University of Delaware
Newark, DE 19716
United States of America
e-mail: coulter@math.udel.edu
marie@math.udel.edu

https://doi.org/10.1017/S0004972700036200 Published online by Cambridge University Press