PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 111, Number 4, April 1991

POWER ROOTS OF LINEARIZED POLYNOMIALS

HAN WEN BAO

(Communicated by William Adams)

ABSTRACT. In the present paper, we have discussed the number of power roots of linearized polynomials. For some cases, the exact formulas are given.

A polynomial of the form

$$L(x) = \sum_{i=0}^{n} a_i x^{p^i}$$

with coefficients a_i in a finite field $\mathrm{GF}(p)$ is called a p-polynomial, it is customary to speak of linearized polynomials. In this paper, we discuss the roots of $L(x^r)$ (also $y^r = L(x)$) in $\mathrm{GF}(p^m)$. The case of $L(x) = x + x^p + \cdots + x^{p^{m-1}}$ is considered in [5, 8].

First we introduce a few definitions.

1. For linearized polynomials $L_1(x)$, $L_2(x)$, we define the symbolic multiplication $\otimes$ by

$$L_1(x) \otimes L_2(x) = L_1(L_2(x)).$$

2. The polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$, $f^*(x) = \sum_{i=0}^{n} a_i x^{p^i}$ over $\mathrm{GF}(p)$ are called p-associates of each other.

If $f_1(x), f_2(x) \in \mathrm{GF}(p)[x]$, we can easily check

$$(*) \qquad (f_1(x) f_2(x))^* = f_1^*(x) \otimes f_2^*(x).$$

Therefore the set of p-polynomials over $\mathrm{GF}(p)$ forms an integral domain under the symbolic multiplication and ordinary addition (for details see [4]), and the symbolic multiplication and ordinary multiplication are related by $(*)$.

For a polynomial $f(x) = \sum a_i x^i \in \mathrm{GF}(p)[x]$, let $d(x) = (f(x), x^m - 1)$, then $f^*(x)$ and $d^*(x)$ have the same set of roots in $\mathrm{GF}(p^m)$. So later we always suppose $f(x) | x^m - 1$. If $\mathrm{GF}(p^m)$ is considered a vector space over $\mathrm{GF}(p)$, $f^*(x)$ induces a linear operator on $\mathrm{GF}(p^m)$. $f^*(\mathrm{GF}(p^m)) = \{f^*(c) | c \in \mathrm{GF}(p^m)\}$ is an additive subgroup of $\mathrm{GF}(p^m)$.

Let G be a finite Abelian group. By a character of G, we mean a group homomorphism $G \to C^*$, where C^* is the multiplicative group of the complex

Received by the editors October 13, 1989 and, in revised form, January 22, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11T30, 12E20.

number field. The characters form an Abelian group $G^{\frown}$, called the dual of G (for the basic properties of characters, see [2]). The dual of the additive group of $\mathrm{GF}(p^m)$ is

$$\mathrm{GF}(p^m)^{\frown} = \{\chi_u | u \in \mathrm{GF}(p^m)\},$$

where $\chi_u(c) = e^{2\pi i T(uc)}$, $c \in \mathrm{GF}(p^m)$, $T(x) = x + x^p + \cdots + x^{p^{m-1}}$ is the absolute trace of $\mathrm{GF}(p^m)$ to $\mathrm{GF}(p)$. We denote the dual of the multiplicative group $\mathrm{GF}(p^m)^*$ of $\mathrm{GF}(p^m)$ by $\mathrm{GF}(p^m)^{*\frown}$.

For every χ_u, its restriction on $f^*(\mathrm{GF}(p^m))$ induces a character $\chi_u{:}$ of $f^*(\mathrm{GF}(p^m))$. We have

Lemma 1. *The map* $\phi : \chi_u \to \chi_u{:}$ *is a surjective homomorphism of* $\mathrm{GF}(p^m)^{\frown}$ *to*

$$f^*(\mathrm{GF}(p^m))^{\frown} \cdot \ker(\phi) = \{\chi_u | f_0^*(u) = 0,\ u \in \mathrm{GF}(p^m)\},$$

where $f_0(x) = x^n f(x^{-1})$, *the reciprocal polynomial of* $f(x)$.

Proof. It is obvious that ϕ is a homomorphism, which is surjective, since every character in $f^*(\mathrm{GF}(p^m))^{\frown}$ can be extended to a character in $\mathrm{GF}(p^m)^{\frown}$.

Let $\chi_u \in \ker(\phi)$. Then $\chi_u(u) = 1$ for $u \in f^*(\mathrm{GF}(p^m))$, i.e. $\chi_u(f^*(c')) = 1$. Hence $T(uf^*(c')) = 0$, for $c' \in \mathrm{GF}(p^m)$. Therefore $\sum_{i=0}^{m-1}(uf^*(x))^{p^i} \equiv 0 \mod x^{p^m} - x$, i.e.

$$\begin{aligned}
\sum_{i=0}^{m-1} u^{p^i} f^*(x^{p^i}) &\equiv \sum_{i=0}^{m-1} u^{p^i} \sum_{j=0}^{n} a_j x^{p^{i+j}} \\
&\equiv \sum_{i=0}^{m-1} \sum_{j=0}^{n} u^{p^i} a_j x^{p^{i+j}} \\
&\equiv x \sum_{j+i\equiv 0 \bmod m} u^{p^i} a_j + x^p \sum_{j+i\equiv 1 \bmod m} u^{p^i} a_j + \cdots + x^{p^{m-1}} \\
&\quad \times \sum_{j+i\equiv m-1 \bmod m} u^{p^i} a_j \\
&\equiv 0 \mod x^{p^m} - x.
\end{aligned}$$

The equation above holds if and only if

$$\sum_{j+i\equiv t \bmod m} u^{p^i} a_j = 0, \qquad t = 0, 1, \ldots, m-1. \tag{1}$$

From this, we see that (1) holds if and only if

$$\sum_{j+i\equiv 0 \bmod m} u^{p^i} a_j = \left(\sum_{j=0}^{n} u^{p^{n-j}} a_j\right)^{p^{m-n}},$$

i.e. $\sum_{j=0}^{n} u^{p^{n-j}} a_j = 0$. So u is a root of $f_0^*(x)$. □

Now let $R(f^*)$ denote the set of the roots of f^*; then $R(f^*)$ is an additive subgroup of $\mathrm{GF}(p^m)$.

Lemma 2. *Let* $g(x) = (x^m - 1)/f(x)$.

(i) $R(g^*) = f^*(\mathrm{GF}(p^m))$.

(ii) *Additive group of* $\mathrm{GF}(p^m) = R(f^*) + R(g^*)$ *if* $(f(x), g(x)) = 1$ (*here the sum is direct sum*).

Remark. If $(m, p) = 1$, $x^m - 1$ does not have multiple factors and $(f(x), g(x)) = 1$.

Proof. (i) Let $f^*(c) \in f^*(\mathrm{GF}(p^m))$, then

$$g^*(f^*(c)) = (fg)^*(c) = (x^m - 1)^*(c) = 0.$$

So $f^*(c) \in R(g^*)$, $R(g^*)$ contains $f^*(\mathrm{GF}(p^m))$. Also $p^{m-n} = |R(g^*)| = |f^*(\mathrm{GF}(p^m))|$, and hence $R(g^*) = f^*(\mathrm{GF}(p^m))$.

(ii) Let $c \in R(f^*) \cap R(g^*)$. Since $(f(x), g(x)) = 1$, there exist $f_1(x)$, $g_1(x)$ such that $f(x)f_1(x) + g(x)g_1(x) = 1$ and $f^*(x) \otimes f_1^*(x) + g^*(x) \otimes g_1^*(x) = x$. So $c = 0$, $R(f^*) \cap R(g^*) = \{0\}$. But $p^m = |R(f^*)||R(g^*)|$, and therefore (ii) holds. □

From now on, we always suppose $(f(x), g(x)) = 1$.

Lemma 3. *Let* $f(x)$, $g(x)$ *be in Lemma* 2, $(f(x), g(x)) = 1$. *Then*

$$f^*(\mathrm{GF}(p^m))^\wedge = \{\chi_u : |u \in R(g_0^*(x))\}.$$

Proof. If $\chi_u := \chi_c :$, then $u - c \in R(f_0^*)$ by Lemma 1, $u - c = 0$. So the set on the right has $|R(g_0^*)|$ elements. Also $|f^*(\mathrm{GF}(p^m))^\wedge| = |f^*(\mathrm{GF}(p^m))| = |R(g^*)| = |R(g_0^*)|$, so Lemma 3 holds. □

Lemma 4. *Let* $c \in \mathrm{GF}(p^m)$. *Then*

$$\sum_u \chi_u(c) = \begin{cases} p^{m-n} & \text{if } f^*(c) = 0, \\ 0 & \text{if } f^*(c) \neq 0, \end{cases}$$

where the sum is taken over $R(g_0^*)$.

Proof. By Lemma 2, $c = c_1 + c_2$, $c_1 \in R(g^*)$, $c_2 \in R(f^*)$, then $\chi_u(c_2) = 1$ by Lemmas 1 and 3. Hence

$$\sum_u \chi_u(c) = \sum_u \chi_u(c_1) = \begin{cases} p^{m-n} & \text{if } c_2 = 0, \\ 0 & \text{if } c_2 \neq 0. \end{cases}$$

This is the reformulation of Lemma 4. □

Now let ψ be a multiplicative and χ an additive character of $\mathrm{GF}(p^m)$. Then the Gaussian sum is defined by

$$G(\psi, \chi) = \sum_{c \in \mathrm{GF}(p^m)} \psi(c)\chi(c).$$

There are many important results on Gaussian sums. Here we give one from the Stickelberg theorem as a lemma.

Lemma 5 [8]. *Let* ψ *be an* r*th order multiplicative character of* $\mathrm{GF}(p^{2ab})$, $r|p^a+1$. *Then*

$$G(\psi, \chi_1) = \begin{cases} (-1)^{b-1}p^{ab} & \text{if } r \text{ odd or } (p^a+1)/r \text{ even,} \\ (-1)^{b-1+bj}p^{ab} & \text{if } r \text{ even and } (p^a+1)/r \text{ odd,} \end{cases}$$

$j = 1, 2, \ldots, r-1$. □

For the subset S of $\mathrm{GF}(p^m)$, let $N_r(S) = |\{c \in \mathrm{GF}(p^m) | c^r = s, s \in S\}|$. If $S = \{s\}$, we denote the number by $N_r(s)$.

Lemma 6 [2]. *Let* ψ *be an* r*th order multiplicative character of* $\mathrm{GF}(p^m)$, $c \in \mathrm{GF}(p^m)$. *Then*

$$N_r(c) = \sum_{j=0}^{r-1} \psi^j(c). \quad \square$$

Now we can give the following result which interprets the relationship between $N_r(R(f^*))$ and $N_r(c^\frown R(g_0^*))$ for some $c^\frown \in \mathrm{GF}(p^m)$.

Theorem 1. *Let* $f(x) = \sum a_i x^i \in \mathrm{GF}(p)(x)$, $r|p^a+1$, $g_0(x)$ *be the reciprocal polynomial of* $g(x) = x^m - 1/f(x)$, $(f(x), g(x)) = 1$. *Then*

$$N_r(R(f^*)) = p^n + (-1)^b p^{ab} + (-1)^{b-1} p^{n-ab} N_r(c^\frown R(g_0^*)),$$

where $c^\frown \in \mathrm{GF}(p^m)$ *and such that*: (1) $c^\frown = 1$ *if* r *odd or* $p^a + 1/r$ *even or* b *even, and* (2) $\psi(c^\frown) = -1$ *otherwise.*

Proof. Let ψ be a rth order multiplicative character of $\mathrm{GF}(p^{2ab})$. By Lemmas 4 and 6, we have

$$\begin{aligned} N_r(R(f^*)) &= p^{-(2ab-n)} \sum_{c \in \mathrm{GF}(p^m)^*} \sum_{j=0}^{r-1} \sum_{u \in R(g_0^*)} \psi^j(c)\chi_u(c) + 1 \\ &= p^{-(2ab-n)} \sum_{j=0}^{r-1} \sum_{u \in R(g_0^*)} G(\psi^j, \chi_u) + 1 \\ &= p^{-(2ab-n)} \left\{ p^{2ab} - 1 + \sum_{j=1}^{r-1} G(\psi^j, \chi_0) + \sum_{u \in R(g_0^*) \setminus \{0\}} G(\psi^0, \chi_u) \right. \\ &\qquad \left. + \sum_{j=1}^{r-1} \sum_{u \in R(g_0^*) \setminus \{0\}} G(\psi^j, \chi_u) \right\} + 1, \end{aligned}$$

where

$$\sum_{j=1}^{r-1} G(\psi^j, \chi_0) = 0, \qquad \sum_{u \in R(g_0^*) \setminus \{0\}} G(\psi^0, \chi_u) = -p^{(2ab-n)} + 1,$$

if r is odd or p^a+1/r even or b even; then, by Lemma 5,

$$\begin{aligned} \text{the last term} &= \sum_{j=1}^{r-1} \sum_{u\in R(g_0^*)\backslash\{0\}} G(\psi^j, \chi_u) \\ &= \sum_{j=1}^{r-1} \sum_{u\in R(g_0^*)\backslash\{0\}} \psi^j(u) G(\psi^j, \chi_1) \\ &= \sum_{j=1}^{r-1} \sum_{u\in R(g_0^*)\backslash\{0\}} \psi^j(u)(-1)^{b-1}p^{ab} \qquad (2) \\ &= (-1)^{b-1}p^{ab}\left\{ \sum_{u\in R(g_0^*)\backslash\{0\}} \sum_{j=0}^{r-1} \psi^j(u) - p^{2ab-n}+1 \right\} \\ &= (-1)^{b-1}p^{ab}\{N_r(R(g_0^*)) - p^{2ab-n}\} \end{aligned}$$

if r even, p^a+1/r odd and b odd, and similarly

$$\text{the last term} = (-1)^{b-1}p^{ab}\{N_r(c^\frown R(g_0^*)) - p^{2ab-n}\};$$

here $c^\frown \in \mathrm{GF}(p^m)$ such that $\psi(c^\frown) = -1$. Collecting the results above, we prove the theorem. $\square$

Let $f(x)\in \mathrm{GF}(p^m)[x]$, $f(0)\neq 0$. The least integer e such that $f(x)|x^e-1$ is called the order of $f(x)$. The least integer e such that $f(x)|x^e+1$ is called the suborder of $f(x)$. Now we give several applications of Theorem 1.

Theorem 2. *Let $f(x)\in \mathrm{GF}(p)[x]$, $f(0)\neq 0$, $\deg(f(x))=n$, the order of $g(x)$ be e, $(f(x), g(x))=1$, $r|p^a+1$. If $r|(p^{2ab}-1)/(p^e-1)$, then the number of the roots of $f^*(x^r)$ in $\mathrm{GF}(p^{2ab})$*

$$N_r(R(f^*)) = p^n + (-1)^{b-1}\delta(r, b)p^{n-ab}(p^{2ab-n}-1); \qquad (3)$$

here

$$\delta(r,b) = \begin{cases} r-1 & \text{if } r \text{ odd or } p^a+1/r \text{ even or } b \text{ even,} \\ -1 & \text{if } r \text{ even, } p^a+1/r \text{ odd and } b \text{ odd.} \end{cases}$$

Proof. Since $f(x)|x^e-1$, $f^*(x)|x^{p^e}-x$, $R(f^*)\subseteq \mathrm{GF}(p^e)$. Suppose η is a primitive root of $\mathrm{GF}(p^{2ab})$. Then $\zeta=\eta^s$ is a primitive root of $\mathrm{GF}(p^e)$; here $s=(p^{2ab}-1)/(p^e-1)$, and hence $\psi(\zeta)=1$. For $c\in \mathrm{GF}(p^e)$, so for $c\in R(f^*)$, $\psi(c)=1$. Now by (2), we can directly get the desired result. $\square$

Corollary 1. *Suppose $(p, 2ab)=1$, $r|p^a+1$.*

(i) *Let $f(x)=(x^{2ab}-1)/(x-1)$. Then*

$$N_r(R(f^*)) = p^{2ab-1} + (-1)^{b-1}\delta(r, b)p^{ab-1}(p-1);$$

here $\delta(r, b)$ is the one in Theorem 2.

(ii) *Let the order of* $g(x)$ *be* q, *an odd prime number,* $\deg(f(x)) = n$. *Then*

$$N_r(R(f^*)) = p^n + (-1)^{b-1}\delta(r, b)p^{n-ab}(p^{2ab-n} - 1);$$

here $\delta(r, b)$ *as before.*

Proof. We only need to prove $r|(p^{2ab} - 1)/(p - 1)$. It holds because

$$(p^{2ab} - 1)/(p - 1) = ((p^{2ab} - 1)/(p^{2a} - 1))((p^a - 1)/(p - 1))(p^a + 1)$$

and

$$((p^{2ab} - 1)/(p^{2a} - 1))((p^a - 1)/(p - 1))$$

is an integer. So (i) holds.

For (ii), we must have $q|ab$ because q is the order of $g(x)$. If $q|a$,

$$(p^{2ab} - 1)/(p^q - 1) = ((p^{2ab} - 1)/(p^{2a} - 1))((p^a - 1)/(p^q - 1))(p^a + 1).$$

If $q \nmid a$, then $(q, 2a) = 1$ and $(p^{2a} - 1, p^q - 1) = p - 1$. Hence

$$(p^{2ab} - 1)(p^a - 1)/(p^{2a} - 1)(p^q - 1)$$

is an integer. Also

$$(p^{2ab} - 1)/(p^q - 1) = \{(p^{2ab} - 1)(p^a - 1)/(p^{2a} - 1)(p^q - 1)\}(p^a + 1),$$

so $r|(p^{2ab} - 1)/(p^q - 1)$. □

Remark. For $q = 2$, $f(x) = (x^{2ab} - 1)/(x^2 - 1)$. If a or b even or $(p+1, r) = 1$, we also have that (ii) holds.

With the application of (ii), e.g., suppose $f(x) = (x^{2ab} - 1)/(x^2 + x + 1)$, $3|ab$, then $N_r(R(f^*)) = p^{2ab-2} + (-1)^{b-1}\delta(r, b)p^{ab-2}(p^2 - 1)$.

Theorem 3. *Let* $f(x) \in \mathrm{GF}(p)[x]$, $f(0) \neq 0$, $\deg(f(x)) = n$, *the suborder of* $g(x)$ *be* e, $(f(x), g(x)) = 1$, $r|p^a + 1$. *If* $r|p^{2ab} - 1/p^e - 1$, *then the number of the roots of* $f^*(x^r)$

$$N_r(R(f^*)) = p^n + (-1)^{b-1}\varepsilon(r, b)p^{n-ab}(p^{2ab-n} - 1); \tag{4}$$

here if $r|p^{2ab} - 1/2(p^e - 1)$, $\varepsilon(r, b) = \delta(r, b)$; *if* $r \nmid (p^{2ab} - 1)/2(p^e - 1)$,

$$\varepsilon(r, b) = \begin{cases} -1 & \text{if } r \text{ odd or } p^a + 1/r \text{ even or } b \text{ even,} \\ r - 1 & \text{if } r \text{ even, } p^a + 1/r \text{ odd and } b \text{ odd.} \end{cases}$$

Proof. First we must have $e|ab$. Let η is a primitive root of $\mathrm{GF}(p^{2ab})$. The roots of $x^{2(p^e-1)} - 1 = 0$ form a cyclic subgroup E of generator $\zeta = \eta^t$ with $2(p^e - 1)$ elements; here $t = (p^{2ab} - 1)/2(p^e - 1)$. ψ induces a character of E. So if $r|(p^{2ab} - 1)/2(p^e - 1)$, then for $c \in E$, $\psi(c) = 1$, similar as Theorem 2; if $2r \nmid (p^{2ab} - 1)/2(p^e - 1)$, ψ induces a quadratic character of E. $\psi(c) = 1$, $c \in \mathrm{GF}(p^e)^*$; $\psi(c) = -1$, $c \in R((x^e + 1)^*)$, $c \neq 0$. Using this result to the proof of Theorem 1, we prove this case. □

Corollary 2. *Suppose* $(p, 2ab) = 1$, $r|p^a + 1$.

(i) *Let* $f(x) = (x^{2ab} - 1)/(x+1)$. *Then*

$$N_r(R(f^*)) = p^{2ab-1} + (-1)^{b-1}\tau(r, b)p^{ab-1}(p-1).$$

Here $\tau(r, b) = \delta(r, b)$ *if* a *or* b *even*; $r-1$ *otherwise.*

(ii) *Let the suborder of* $g(x)$ *be* q, *an odd prime number,* $\deg(f(x)) = n$. *Then*

$$N_r(R(f^*)) = p^n + (-1)^{b-1}\tau(r, b)p^{n-ab}(p^{2ab-n} - 1);$$

here $\tau(r, b)$ *as* (i).

Proof. Following the proof of Corollary 1, we have

$$(p^{2ab} - 1)/(p-1) = ((p^{2ab} - 1)/(p^{2a} - 1))((p^a - 1)/(p-1))(p^a + 1)$$

and

$$((p^{2ab} - 1)/(p^{2a} - 1))((p^a - 1)/(p-1))$$

is an integer. If a or b is even, $r|(p^{2ab} - 1)/2(p-1)$ and

$$N_r(R(f^*)) = p^{2ab-1} + (-1)^{b-1}\delta(r, b)p^{ab-1}(p-1);$$

if a and b are odd, $r|(p^{2ab} - 1)/2(p^e - 1)$ if and only if $p^a + 1/r$ even and

$$N_r(R(f^*)) = p^{2ab-1} + (-1)^{b-1}(r-1)p^{ab-1}(p-1).$$

Similarly, from the proof of Corollary 1 we see that if a or b even, then $r|(p^{2ab} - 1)/2(p-1)$ and

$$N_r(R(f^*)) = p^n + (-1)^{b-1}\delta(r, b)p^{ab-n}(p^{2ab-n} - 1);$$

if a and b odd, $r|(p^{2ab} - 1)/2(p^e - 1)$ if and only if $p^a + 1/r$ even and

$$N_r(R(f^*)) = p^n + (-1)^{b-1}(r-1)p^{ab-n}(p^{2ab-n} - 1). \quad \square$$

Remark. When q is a composite number, we can use (3) or (4) to obtain some partial results.

In fact, by Lemma 2, we also obtain the number of roots of $y^r = g^*(x)$ in $\mathrm{GF}(p^{2ab})$.

Acknowledgment

The author is very grateful to the referee for his comments.

References

1. H. Davenport, *Bases for finite fields*, J. London Math. Soc. **43** (1968), 21–39.
2. K. Irland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, Heidelberg, and Berlin, 1982.
3. H. W. Lenstra, Jr. and R. J. Schoof, *Primitive normal bases for finite fields*, Math. Comp. **48** (1987), 217–231.
4. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.
5. O. Moreno, *Counting trace of powers over* $\mathrm{GF}(2^m)$, Congr. Numer. **29** (1980), 673–679.

6. O. Ore, *Contributions to the theory of finite fields,* Trans. Amer. Math. Soc. **36** (1934), 243–274.
7. H. Wenbao, *On counting absolute trace of powers in* $\mathrm{GF}(p^m)$, Acta Math. Sinica **4** (1988), 266–269.

DEPARTMENT OF MATHEMATICS, SICHUAN UNIVERSITY, CHENG DU, PEOPLE'S REPUBLIC OF CHINA