JOURNAL OF NUMBER THEORY 7, 361–365 (1975)

Note on Cubics over $GF(2^n)$ and $GF(3^n)$*

KENNETH S. WILLIAMS

Department of Mathematics, Carleton University, Ottawa, Canada K1S 5B6

Communicated by S. Chowla

Received March 27, 1972

A description of the factorization of a cubic polynomial over the fields $GF(2^n)$ and $GF(3^n)$ is given. The results are analogous to those given by Dickson for a cubic over $GF(p^n), p > 3$.

1. INTRODUCTION

A description of the factorization of a cubic polynomial over the field $GF(p^n)$ has been given by Dickson [4] when the characteristic p of the field is >3. As $p \neq 3$ it is clear that we need only consider cubics $f(x)$ of the form $x^3 + ax + b$, where $a, b \in GF(p^n)$. Further f has no squared factors if discrim $(f) = -4a^3 - 27b^2 \neq 0$. If f factors over $GF(p^n)$ as a product of three linear factors we write $f = (1, 1, 1)$, if f factors as a product of a linear factor and an irreducible quadratic factor we write $f = (1, 2)$, and finally if f is itself irreducible over $GF(p^n)$ we write $f = (3)$. Denoting a root of $y^2 = -3$ by w, so that $w \in GF(p^n)$ if $p^n \equiv 1 \pmod 3$ and $w \in GF(p^{2n})$ if $p^n \equiv 2 \pmod 3$, we can state Dickson's theorem as follows:

THEOREM (Dickson). *The factorizations of $f(x) = x^3 + ax + b$ ($a, b \in GF(p^n)$, $p > 3$, $-4a^3 - 27b^2 \neq 0$) over $GF(p^n)$ are characterized as follows*:

$$f = (1, 1, 1) \Leftrightarrow -4a^3 - 27b^2 \text{ is a square in } GF(p^n), \tag{1.1}$$

say $-4a^3 - 27b^2 = 81c^2$, *and* $1/2(-b + cw)$ *is a cube in* $GF(p^n)$ (*if* $p^n \equiv 1 \pmod 3$), $GF(p^{2n})$ (*if* $p^n \equiv 2 \pmod 3$),

$$f = (1, 2) \Leftrightarrow -4a^3 - 27b^2 \text{ is not a square in } GF(p^n), \tag{1.2}$$

$$f = (3) \Leftrightarrow -4a^3 - 27b^2 \text{ is a square in } GF(p^n), \tag{1.3}$$

* Research partially supported by National Research Council of Canada (Grant A-7233).

say $-4a^3 - 27b^2 = 81c^2$, *and* $1/2(-b + cw)$ *is not a cube in* $GF(p^n)$ (*if* $p^n \equiv 1 \pmod 3$)), $GF(p^{2n})$ (*if* $p^n \equiv 2 \pmod 3$)).

In this note we obtain analogous results for cubics over $GF(2^n)$ and $GF(3^n)$. We make use of Stickelberger's theorem for both even and odd characteristics (see for example [1, pp. 159–171] and the well-known result that the polynomial $x^2 + bx + c$, $b\ (\neq 0)$ and $c \in GF(2^n)$, is reducible over $GF(2^n)$ if and only $\mathrm{tr}(c/b^2) = 0$, where for $\lambda \in GF(2^n)$, $\mathrm{tr}(\lambda) = \lambda + \lambda^2 + \lambda^{2^2} + \cdots + \lambda^{2^{n-1}}$ denotes the trace of λ over $GF(2)$ (see for example [3, p. 555]).

2. Factorizations Over $GF(2^n)$

Clearly we may take $f(x) = x^3 + ax + b$, where $a, b \in GF(2^n)$ and $b \neq 0$. We let t_1, t_2 denote the roots of $t^2 + bt + a^3 = 0$, so that t_1, t_2 lie in $GF(2^n)$, if $\mathrm{tr}(a^3/b^2) = 0$, and in $GF(2^{2n})$, if $\mathrm{tr}(a^3/b^2) = 1$. As $t_1t_2 = a^3$, t_1, t_2 are both cubes or both not cubes in $GF(2^n)$ (if $\mathrm{tr}(a^3/b^2) = 0$), $GF(2^{2n})$ (if $\mathrm{tr}(a^3/b^2) = 1$). We prove

THEOREM 1. *The factorizations of* $f(x) = x^3 + ax + b$ ($a, b \in GF(2^n)$, $b \neq 0$) *over* $GF(2^n)$ *are characterized as follows*:

$$f = (1, 1, 1) \Leftrightarrow \mathrm{tr}(a^3/b^2) = \mathrm{tr}(1),\ t_1, t_2 \textit{ cubes in } GF(2^n)\ (n \textit{ even}),\ GF(2^{2n})\ (n \textit{ odd}), \tag{2.1}$$

$$f = (1, 2) \Leftrightarrow \mathrm{tr}(a^3/b^2) \neq \mathrm{tr}(1), \tag{2.2}$$

$$f = (3) \Leftrightarrow \mathrm{tr}(a^3/b^2) = \mathrm{tr}(1),\ t_1, t_2 \textit{ not cubes in } GF(2^n)\ (n \textit{ even}),\ GF(2^{2n})\ (n \textit{ odd}). \tag{2.3}$$

Proof. By Stickelberger's theorem ([1, p. 169]) f has an even number of irreducible factors over $GF(2^n)$ if and only if $\mathrm{tr}(1 + a^3/b^2) = 1$, that is, $f = (1, 2)$ if and only if $\mathrm{tr}(a^3/b^2) \neq \mathrm{tr}(1)$. This proves (2.2). To complete the proof it suffices to prove (2.1).

If $f = (1, 1, 1)$ then by Stickelberger's theorem we have $\mathrm{tr}(1 + a^3/b^2) = 0$, that is $\mathrm{tr}(a^3/b^2) = \mathrm{tr}(1)$. Suppose however t_1, t_2 are not cubes in $GF(2^n)$ (if n even), $GF(2^{2n})$ (if n odd). Let t denote one of t_1, t_2 and define θ by $\theta^3 = t$ so that

$$\begin{cases} \theta \in GF(2^{3n}), & \theta \notin GF(2^n), \quad \text{if } n \text{ even}, \\ \theta \in GF(2^{6n}), & \theta \notin GF(2^{2n}), \quad \text{if } n \text{ odd}. \end{cases} \tag{2.4}$$

Now

$$\left(\theta + \frac{a\theta^2}{t}\right)^3 + a\left(\theta + \frac{a\theta^2}{t}\right) + b = 0,$$

so that as $f = (1, 1, 1)$ we have $\theta + a\theta^2/t \in GF(2^n)$. But $t \in GF(2^n)$ (if n even), $GF(2^{2n})$ (if n odd), so that we have $\theta \in GF(2^{2n})$ (if n even), $GF(2^{4n})$ (if n odd), which contradicts (2.4).

Now suppose that $\mathrm{tr}(a^3/b^2) = \mathrm{tr}(1)$ and t_1, t_2 are cubes in $GF(2^n)$ (if n even), $GF(2^{2n})$ (if n odd). If $f \neq (1, 1, 1)$ then as $\mathrm{tr}(a^3/b^2) = \mathrm{tr}(1)$ (so that $f \neq (1, 2)$) we must have f irreducible over $GF(2^n)$. Letting t denote one of t_1, t_2 we see that there exists $u \in GF(2^n)$ (n even), $GF(2^{2n})$ (n odd), such that $t = u^3$. As $t^2 + bt + a^3 = 0$ we have $u^6 + bu^3 + a^3 = 0$ and so $(u + a/u)^3 + a(u + a/u) + b = 0$, that is, f has a root in $GF(2^n)$ (if n even), $GF(2^{2n})$ (if n odd), contradicting that f is irreducible over $GF(2^n)$.

We remark that part of this theorem (namely (2.2)) is given in [3, p. 556], and that a different characterization is given in [2].

3. Factorizations Over $GF(3^n)$

We begin by proving the following lemma.

Lemma. *The factorizations of* $x^3 - x + c$ $(c \in GF(3^n))$ *over* $GF(3^n)$ *are characterized as follows:*

$$x^3 - x + c = (1, 1, 1) \Leftrightarrow \mathrm{tr}(c) = 0 \tag{3.1}$$

and

$$x^3 - x + c = (3) \Leftrightarrow \mathrm{tr}(c) \neq 0, \tag{3.2}$$

where $\mathrm{tr}(c) = c + c^3 + c^{3^2} + \cdots + c^{3^{n-1}}$.

Proof. As discrim $(x^3 - x + c) = -4(-1)^3 - 27c^2 = 2^2$, by Stickelberger's theorem [1, p. 164] we have $x^3 - x + c \neq (1, 2)$. Moreover it has no squared factor. Hence $x^3 - x + c = (1, 1, 1)$ or (3), and it suffices to prove (3.1).

We let

$$V_1 = \{c \in GF(3^n) \mid \mathrm{tr}(c) = 0\},$$
$$V_2 = \{c \in GF(3^n) \mid x^3 - x + c = (1, 1, 1)\}.$$

If $c \in V_2$ there exists $x_1 \in GF(3^n)$ such that $x_1^3 - x_1 + c = 0$, that is

$$\begin{aligned} \operatorname{tr}(c) = \operatorname{tr}(x_1^3 - x_1) &= \operatorname{tr}(x_1^3) - \operatorname{tr}(x_1) \\ &= (x_1^3 + x_1^9 + \cdots + x_1^{3^n}) \\ &\quad - (x_1 + x_1^3 + \cdots + x_1^{3^{n-1}}) \\ &= x_1^{3^n} - x_1 = 0, \end{aligned}$$

implying $c \in V_1$, that is $V_2 \subseteq V_1$.

If $c_1, c_2 \in V_1$ and $\lambda \in GF(3)$ then

$$\operatorname{tr}(c_1 + c_2) = \operatorname{tr}(c_1) + \operatorname{tr}(c_2) = 0, \qquad \operatorname{tr}(\lambda c) = \lambda \operatorname{tr}(c) = 0,$$

so that V_1 is a subspace of $GF(3^n)$ considered as a vector space (of dimension n) over $GF(3)$. Since $\operatorname{card}(V_1) = 3^{n-1}$ we have $\dim V_1 = n - 1$.

If $c_1, c_2 \in V_2$ and $\lambda \in GF(3)$ then there exist $x_1, x_2 \in GF(3^n)$ such that

$$\begin{aligned} &(x_1 + x_2)^3 - (x_1 + x_2) + (c_1 + c_2) \\ &\quad = (x_1^3 - x_1 + c_1) + (x_2^3 - x_2 + c_2) = 0 \end{aligned}$$

and (as $\lambda^3 = \lambda$) $(\lambda x_1)^3 - (\lambda x_1) + \lambda c_1 = \lambda(x_1^3 - x_1 + c_1) = 0$, implying V_2 is also a subspace of the vector space $GF(3^n)$ over $GF(3)$. Since $\operatorname{card}(V_2) = 3^{n-1}$ we have $\dim V_2 = n - 1$.

Hence we have $V_2 \subseteq V_1$, $\dim V_1 = \dim V_2$, proving $V_1 = V_2$ as required.

We are now in a position to treat the factorization of a general cubic $g(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$ over $GF(3^n)$. If $a_2 = 0$ we work with $(1/a_3)\, g(x)$. If $a_2 \neq 0$ we work with $(x^3/a_3)\, g(1/x + a_1/a_2)$.

In both cases the factorization of $g(x)$ can be retrieved, and so it suffices to consider $f(x) = x^3 + ax + b$ $(a, b \in GF(3^n))$. Moreover since the factorization of $x^3 + b$ over $GF(3^n)$ is well-known we can further take $a \neq 0$. We prove

THEOREM 2. *The factorizations of $f(x) = x^3 + ax + b$ $(a, b \in GF(3^n)$, $a \neq 0)$ over $GF(3^n)$ are characterized as follows:*

$$f = (1, 1, 1) \Leftrightarrow -a \text{ is a square in } GF(3^n), \tag{3.3}$$

say $-a = c^2$, and $\operatorname{tr}(b/c^3) = 0$,

$$f = (1, 2) \Leftrightarrow -a \text{ not a square in } GF(3^n), \tag{3.4}$$

$$f = (3) \Leftrightarrow -a \text{ is a square in } GF(3^n), \tag{3.5}$$

say $-a = c^2$, and $\operatorname{tr}(b/c^3) \neq 0$.

Proof. (3.4) follows immediately from Stickelberger's theorem [1, p. 164]. Hence we can suppose there exists $c \in GF(3^n)$ such that $-a = c^2$ so that $f(x) = x^3 - c^2x + b$. We set $f^*(x) = x^3 - x + b/c^3$ and note that as $f(cx) = c^3 f^*(c)$, f and f^* factor in the same way over $GF(3^n)$. Hence by the lemma we have $f = (1, 1, 1) \Leftrightarrow g = (1, 1, 1) \Leftrightarrow \operatorname{tr}(b/c^3) = 0$, which completes the proof of Theorem 2.

4. Remark

We remark that similar results for quartic polynomials over $GF(p^n)$ $(p > 2)$ can be deduced from [5] (see also [4, 7]) and over $GF(2^n)$ the results are given in [6].

References

1. E. R. Berlekamp, "Algebraic Coding Theory," McGraw-Hill, 1968.
2. E. R. Berlekamp, H. Rumsey, and G. Solomon, Solutions of algebraic equations in fields of characteristic 2, Jet Propulsion Lab. Space Programs Summary No. 4, 37–39, 1966.
3. E. R. Berlekamp, H. Rumsey, and G. Solomon, On the solution of algebraic equations over finite fields, *Inform. Contr.* **10** (1967), 553–564.
4. L. E. Dickson, Criteria for the irreducibility of functions in a finite field, *Bull. Amer. Math. Soc.* **13** (1906), 1–8.
5. P. A. Leonard, On factoring quartics (mod p), *J. Number Theory* **1** (1969), 113–115.
6. P. A. Leonard and K. S. Williams, Quartics over $GF(2^n)$, *Proc. Amer. Math. Soc.* **36** (1972), 347–350.
7. Th. Skolem, The general congruence of 4th degree modulo p, p prime, *Norsk. Mat. Tidsskr.* **34** (1952), 73–80.