The third-order factorable core of polynomials over finite fields

By Javier GOMEZ-CALDERON

Department of Mathematics, The Pennsylvania State University, U. S. A.

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1998)

Abstract: Let $\boldsymbol{F}_q$ denote the finite field of order q and characteristic p. For $f(x)$ in $\boldsymbol{F}_q[x]$, let $f^*(x, y)$ denote the substitution polynomial $f(x)$-$f(y)$. In this paper we show that if $f(x) = x^d + a_{d-2}x^{d-2} + a_{d-3}x^{d-3} + \cdots + a_1x + a_0 \in F_q[x]$ $(a_{d-2}a_{d-3} \neq 0)$ has degree d prime to q and $f^*(x, y)$ has at least one cubic irreducible factor, then

$f(x) = G(x^4 + (4a_{d-2}/d)x^2 + (4a_{d-3}/d)x)$ for some $G(x) \in \boldsymbol{F}_q[x]$

or

$f(x) = H((x^3 + (3a_{d-2}/d)x + 3a_{d-3}/d)^{r+1})$ for some $H(x) \in \boldsymbol{F}_q[x]$

where r denotes the number of irreducible cubic factors of $f^*(x, y)$ of the form $x^3 - Ty^3 + Ax + By + C$.

Let $\boldsymbol{F}_q$ denote the finite field of order q and characteristic p. For $f(x)$ in $\boldsymbol{F}_q[x]$, let $f^*(x, y)$ denote the substitution polynomial $f(x) - f(y)$. The polynomial $f^*(x, y)$ has frequently been used in questions on the values set of $f(x)$, see for example Wan [8], Dickson [4], Hayes [7], and Gomez-Calderon and Madden [6]. Recently in [2] and [3], Cohen and in [1], Acosta and Gomez-Calderon studied the linear and quadratic factors of $f^*(x, y)$. In this paper we consider the irreducible cubic factors of $f^*(x, y)$. We show that if $f(x) = x^d + a_{d-2}x^{d-2} + a_{d-3}x^{d-3} + \cdots + a_1x + a_0 \in \boldsymbol{F}_q[x]$ $(a_{d-2}a_{d-3} \neq 0)$ has degree d prime to q and $f^*(x, y)$ has at least one cubic irreducible factor, then

$$f(x) = G(x^4 + (4a_{d-2}/d)x^2 + (4a_{d-3}/d)x)$$

for some $G(x) \in \boldsymbol{F}_q[x]$

or

$$f(x) = H((x^3 + (3a_{d-2}/d)x + 3a_{d-3}/d)^{r+1})$$

for some $H(x) \in \boldsymbol{F}_q[x]$ where r denotes the number of irreducible cubic factors of $f^*(x, y)$ of the form $x^3 - Ty^3 + Ax + By + C$.

Now we will give a series of lemmas from which our main result, Theorem 7, will follow. Proofs for Lemmas 1 and 2 can be found in [5].

Lemma 1. Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ denote a monic polynomial over $\boldsymbol{F}_q$ of degree d prime to q. Let the irreducible factorization of $f^*(x, y) = f(x) - f(y)$ be given by

$$f^*(x, y) = \prod_{i=1}^{s} f_i(x, y).$$

Let

$$f_i(x, y) = \sum_{j=0}^{n_i} g_{ij}(x, y)$$

be the homogeneous decomposition of $f_i(x, y)$ so that $n_i = \deg(f_i(x, y))$ and $g_{ij}(x, y)$ is homogeneous of degree j. Assume $a_{d-1} = a_{d-2} = \cdots = a_{d-r} = 0$ for some $r \geq 1$. Then

$$g_{in_i-1}(x, y) = g_{in_i-2}(x, y) = \cdots = g_{iR_i}(x, y) = 0$$

where

$$R_i = \begin{cases} n_i - r \text{ if } n_i \geq r \\ 0 \quad \text{if } n_i < r. \end{cases}$$

Lemma 2. Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ be a monic polynomial over $\boldsymbol{F}_q$ of degree d prime to q. Let N be the number of homogeneous linear factors of $f^*(x, y) = f(x) - f(y)$ over $\boldsymbol{F}_{q^r}$ for some $r \geq 1$. Then, $f(x) = g(x^N)$ for some $g(x) \in \boldsymbol{F}_q[x]$.

Lemma 3. Let d denote a positive divisor of $q - 1$. Then

$$\frac{x^{d-r} - y^{d-r}}{x^d - y^d} = \sum_{i=0}^{d-1} \frac{\mu^{-i(r-1)} - \mu^i}{dy^{r-1}(x - \mu^i y)}$$

where μ denotes a d-th primitive root of unity in $\boldsymbol{F}_q$.

Proof. Considering the expressions as rational functions in x over the rational function field $\boldsymbol{F}_q(y)$ we obtain

$$\frac{x^{d-r} - y^{d-r}}{x^d - y^d} = \sum_{i=0}^{d-1} \frac{A_i}{x - \mu^i y},$$

for some $A_0, A_1, \ldots, A_{d-1}$ in $\boldsymbol{F}_q(y)$. Hence,

$$x^{d-r} - y^{d-r} = \sum_{i=0}^{d-1} \prod_{j \neq i} (x - \mu^j y)A_i,$$

$$(\mu^i y)^{d-r} - y^{d-r} = \prod_{j \neq i} (\mu^i y - \mu^j y)A_i,$$