DICKSON CURVES

JAVIER GOMEZ-CALDERON

Received 6 March 2006; Accepted 26 March 2006

Let K_q denote the finite field of order q and odd characteristic p. For $a \in K_q$, let $g_d(x,a)$ denote the Dickson polynomial of degree d defined by $g_d(x,a) = \sum_{i=0}^{[d/2]} d/(d-i)\binom{d-i}{i}(-a)^i x^{d-2i}$. Let $f(x)$ denote a monic polynomial with coefficients in K_q. Assume that $f^2(x)-4$ is not a perfect square and $\gcd(p,d)=1$. Also assume that $f(x)$ and $g_2(f(x),1)$ are not of the form $g_d(h(x),c)$. In this note, we show that the polynomial $g_d(y,1)-f(x) \in K_q[x,y]$ is absolutely irreducible.

Let K_q denote the finite field of order q and odd characteristic p. For $a \in K_q$, let $g_d(x,a)$ denote the Dickson polynomial of degree d and parameter a defined by $g_d(x,a) = \sum_{i=0}^{[d/2]} d/(d-i)\binom{d-i}{i}(-a)^i x^{d-2i}$. Alternatively, $g_d(x,a)$ can also be defined by the second-order linear recursive sequence

$$g_d(x,a) = xg_{d-1}(x,a) - ag_{d-2}(x,a), \tag{1}$$

where $g_o(x,a) = 2$ and $g_1(x,a) = x$. Thus,

$$g_d(x,a) = g_d\left(y + \frac{a}{y}, a\right) = y^d + \frac{a^d}{y^d}, \tag{2}$$

where x and y are related by the *generating equation* $y^2 - xy + a = 0$. Dickson polynomials have been extensively studied by many authors and an excellent survey of their many properties and applications has been written by Lidl et al. [2]. Since $g_d(x,0) = x^d$, the Dickson polynomial $g_d(x,a)$ may be viewed as a generalization of the power polynomial x^d. Equations of the form $y^d = f(x)$ are called *elliptic equations* and have a very rich research history, see, for example, [1, Chapter 18]. In particular, if $f(x) = (x-c_1)^{d_1}\cdots(x-c_s)^{d_s}$ is the factorization of $f(x) \in K_q[x]$ in $\bar{K}_q$, then it is easy to prove that, see [3, page 11], $y^d - f(x) \in K_q[x,y]$ is absolutely irreducible if and only if $\gcd(d,d_1,\dots,d_s) = 1$. Hence, applying Weil's Riemman hypothesis theorem [3, page 131], if $e = \max\{d, \deg(f(x))\}$

Hindawi Publishing Corporation
International Journal of Mathematics and Mathematical Sciences
Volume 2006, Article ID 42818, Pages 1–6
DOI 10.1155/IJMMS/2006/42818

and $\gcd(d, d_1, \dots, d_s) = 1$, then the number of roots N of $y^d - f(x)$ in $K_q \times K_q$ satisfies the inequality

$$|N - q| \le (e-1)(e-2)\sqrt{q} + c(e) \tag{3}$$

for some constant $c(e)$.

In this note, we show that if $\gcd(p,d) = 1$ and $f^2(x) - 4$ is not a perfect square, then $g_d(y,1) - f(x) \in K_q[x,y]$ is absolutely irreducible as far as both $f(x)$ and $g_2(f(x),1)$ are not of the form $g_d(h(x),c)$ for some constant c and $h(x) \in K_q[x]$.

The following lemmas will be needed to prove our main result, Theorem 3.

Lemma 1. *Let K_q denote the finite field of order q and odd characteristic p. Let $f(x)$ be a monic polynomial with coefficients in K_q. Assume that $f^2(x) - 4$ is not a perfect square. Then*

(a) $(f(x) \pm \sqrt{f^2(x) - 4})^n \notin K_q(x)$ *for* $n \ge 1$;

(b) *if* $n \ge 1$ *and* $(f(x) + \sqrt{f^2(x) - 4})^n + c(f(x) - \sqrt{f^2(x) - 4})^n \in \bar{K}_q(x)$, *then* $c = 1$.

Proof. (a) Assume that $(f(x) \pm \sqrt{f^2(x) - 4})^n = \sum_{j=0}^{n} (-1)^j \binom{n}{j} f^{n-j}(x) (\sqrt{f^2(x) - 4})^j \in K_q(x)$. Then

$$h(x) = \sum_{i=0}^{m} \binom{n}{2i+1} f^{n-2i-1}(x) (f(x) - 4)^i = 0, \tag{4}$$

where $m = [(n-1)/2]$. Hence, the leading coefficient of $h(x)$ gives the contradiction $\sum_{i=0}^{m} \binom{n}{2i+1} = 2^{n-1} = 0$. Therefore, $(f(x) \pm \sqrt{f^2(x) - 4})^n \notin K_q(x)$ for $n \ge 1$.

(b) Assume that $(f(x) + \sqrt{f^2(x) - 4})^n + c(f(x) - \sqrt{f^2(x) - 4})^n \in \bar{K}_q(x)$ for some $n \ge 1$. Then

$$\sum_{i=0}^{m} (1-c)(f(x))^{n-2i-1} (f^2(x) - 4)^i = 0, \tag{5}$$

where $m = [(n-1)/2]$. Therefore, $(1-c)\sum_{i=0}^{m} \binom{n}{2i+1} = (1-c)2^{n-1} = 0$ and so $c = 1$. □

Lemma 2. *With notation as in Theorem 3, assume that $\sigma_r(a_1, \dots, a_n)\theta^r + \sigma_r(1/a_1, \dots, 1/a_n)\theta^{-r} \in \bar{K}_q(x)$ for some $r \ge 1$. Then, $\sigma_r(a_1, \dots, a_n) = 0$ if and only if $\sigma_r(1/a_1, \dots, 1/a_n) = 0$.*

Proof. Assume that $\sigma_r(a_1, \dots, a_n) \ne 0$ and $\sigma_r(1/a_1, \dots, 1/a_n) = 0$. Then, $\theta^{dr} = (f(x) + \sqrt{f^2(x) - 4})^r \in \bar{K}_q(x)$ contradicting Lemma 2. A similar argument also shows that the cases $\sigma_r(a_1, \dots, a_n) = 0$ and $\sigma_r(1/a_1, \dots, 1/a_n) \ne 0$ cannot occur. Therefore, $\sigma_r(a_1, \dots, a_n) = 0$ if and only if $\sigma_r(1/a_1, \dots, 1/a_n) = 0$. □

Theorem 3. *Let K_q denote the finite field of order q and odd characteristic p. Let $f(x)$ be a monic polynomial with coefficients in K_q. Assume that $f^2(x) - 4$ is not a perfect square. For $d \ge 1$, let $g_d(y,1)$ denote the Dickson polynomial of degree d and parameter 1. Assume that $f(x)$ and $g_2(f(x),1)$ are not of the form $g_d(h(x),c)$ for some $c \in \bar{K}_q$ and $h(x) \in K_q[x]$. Assume that* $\gcd(p,d) = 1$. *Then, $g_d(y,1) - f(x) \in K_q[x,y]$ is absolutely irreducible.*

Proof. Consider $g_d(y,1) - f(x)$ as a polynomial in y with coefficients in the field of rational functions $\bar{K}_q(x)$. Set $y = w + 1/w$. Then, $g_d(y,1) - f(x) = w^d + 1/w^d - f(x) = 0$ if and only if $w^d = (f(x) \pm \sqrt{f^2(x) - 4})/2$. Hence, combining with Lemma 1,

$$g_d(y,1) - f(x) = \prod_{i=1}^{d}\left(y - \varsigma_d^i\theta - \frac{1}{\varsigma_d^i\theta}\right), \tag{6}$$

where θ is any of the roots of $w^d = (f(x) \pm \sqrt{f^2(x) - 4})/2$.

Now assume that $g_d(y,1) - f(x)$ is reducible over $\bar{K}_q[x,y]$; that is,

$$g_d(y,1) - f(x) = \prod_{i=1}^{r} f_i(x,y) \tag{7}$$

for some polynomials $f_i(x,y) \in \bar{K}_q[x,y]$ with degree in y less than d. Then,

$$f_i(x,y) = \prod_{j=1}^{n_i}\left(y - a_{ij}\theta - \frac{1}{a_{ij}\theta}\right) \in \bar{K}_q[x,y], \tag{8}$$

where $\{a_{i1}, a_{i2}, \dots, a_{in_i}\} \subset \{1, \varsigma_d, \dots, \varsigma_d^{n-1}\}$.

Therefore,

$$\begin{aligned} f_i(x,y) &= \prod_{j=1}^{n_i}\left(y - a_{ij}\theta - \frac{1}{a_{ij}\theta}\right) \\ &= y^{n_i} + h_{i1}(x)y^{n_i-1} + \cdots + h_{in_i-1}(x)y + h_{in_i}(x) \in \bar{K}_q[x,y], \end{aligned} \tag{9}$$

where the polynomials $h_{ij}(x)$ can be expressed in terms of elementary symmetric polynomials as the following equations show:

$$h_{i1}(x) = \sigma_1(a_{i1}, a_{i2}, \dots, a_{in_i})\theta + \sigma_1\left(\frac{1}{a_{i1}}, \frac{1}{a_{i2}}, \dots, \frac{1}{a_{in_i}}\right)\theta^{-1},$$

$$\begin{aligned} h_{i2}(x) = {} & \sigma_2(a_{i1}, \dots, a_{in_i})\theta^2 + \sigma_2\left(\frac{1}{a_{i1}}, \dots, \frac{1}{a_{in_i}}\right)\theta^{-2} \\ & + \sum_{j=1}^{n_i}\left[\frac{\sigma_1(a_{i1}, \dots, \widehat{a}_{ij}, \dots, a_{in_i})}{a_{ij}} + a_{ij}\sigma_1\left(\frac{1}{a_{i1}}, \dots, \frac{\widehat{1}}{a_{ij}}, \dots, \frac{1}{a_{in_i}}\right)\right], \end{aligned}$$

$$\vdots$$

$$
\begin{aligned}
h_{in_i}(x) &= \sigma_{n_i}(a_{i1},\dots,a_{in_i})\theta^{n_i} + \sigma_{n_i}\left(\frac{1}{a_{i1}},\dots,\frac{1}{a_{in_i}}\right)\theta^{-n_i} \\
&\quad + \sum_{j=1}^{n_i}\left[\frac{\sigma_{n_i-1}(a_{i1},\dots,\widehat{a}_{ij},\dots,a_{in_i})\theta^{n_i-2}}{a_{ij}} + a_{ij}\sigma_{n_i-1}\left(\frac{1}{a_{i1}},\dots,\frac{\widehat{1}}{a_{ij}},\dots,\frac{1}{a_{in_i}}\right)\theta^{-n_i+2}\right] \\
&\quad + \sum_{t\neq j}^{n_i}\left[\frac{\sigma_{n_i-2}(a_{i1},\dots,\widehat{a}_{it},\dots,\widehat{a}_{ij},\dots,a_{in_i})\theta^{n_i-4}}{a_{it}a_{ij}}\right. \\
&\qquad\qquad \left. + a_{it}a_{ij}\sigma_{n_i-2}\left(\frac{1}{a_{i1}},\dots,\frac{\widehat{1}}{a_{it}},\dots,\frac{\widehat{1}}{a_{ij}},\dots,\frac{1}{a_{in_i}}\right)\theta^{-n_i+4}\right] \\
&\qquad\qquad \vdots \\
&\quad + \sum_{t_s\neq t_j}^{n_i}\left[\frac{\sigma_{n_i-w}(a_{i1},\dots,\widehat{a}_{it_1},\dots,\widehat{a}_{it_w},\dots,a_{in_i})\theta^{n_i-2w}}{a_{it_1}a_{it_2}\cdots a_{it_w}}\right. \\
&\qquad\qquad \left. + a_{it_1}\cdots a_{it_w}\sigma_{n_i-w}\left(\frac{1}{a_{i1}},\dots,\frac{\widehat{1}}{a_{it_1}},\dots,\frac{\widehat{1}}{a_{it_w}},\dots,\frac{1}{a_{in_i}}\right)\theta^{-n_i+2w}\right],
\end{aligned}
\tag{10}
$$

where $w = [n_i/2]$ and $\deg(h_{ij}(x)) < \deg(f(x))$ for $1 \le j \le n_i$. □

Now, combining with Lemma 2, we consider the following two cases.

Case 1. $\sigma_1(a_{i1},\dots,a_{in_i})\sigma_1(1/a_{i1},\dots,1/a_{in_i}) \neq 0$ for some $1 \le i \le r$. Then,

$$
\theta + c_i\theta^{-1} = \frac{h_{i1}(x)}{c_i} = H_{i1}(x) \in \bar{K}_q[x], \tag{11}
$$

where $c_i = \sigma_1(1/a_{i1},\dots,1/a_{in_i})/\sigma_1(a_{i1},\dots,a_{in_i})$. Hence,

$$
\begin{aligned}
g_d\left(\theta + \frac{c_i}{\theta}, c_i\right) &= \frac{f(x) \pm \sqrt{f^2(x) - 4}}{2} + c_i^d \frac{f(x) \mp \sqrt{f^2(x) - 4}}{2} \\
&= g_d(H_{i1}(x), c_i).
\end{aligned}
\tag{12}
$$

Therefore,

$$
f(x) = g_d(H_{i1}(x), c_i), \tag{13}
$$

where $c_i^d = 1$.

Case 2. $\sigma_1(a_{i1},\dots,a_{in_i}) = \sigma_1(1/a_{i1},\dots,1/a_{in_i}) = 0$ for all $1 \le i \le r$. Then,

$$\begin{aligned} h_{i2}(x) &= \sigma_2(a_{i1},\dots,a_{in_i})\theta^2 + \sigma_2\left(\frac{1}{a_{i1}},\dots,\frac{1}{a_{in_i}}\right)\theta^{-2} \\ &\quad + \sum_{j=1}^{n_i}\left[\frac{\sigma_1(a_{i1},\dots,\hat{a}_{ij},\dots,a_{in_i})}{a_{ij}} + a_{ij}\sigma_1\left(\frac{1}{a_{i1}},\dots,\widehat{\frac{1}{a_{ij}}},\dots,\frac{1}{a_{in_i}}\right)\right] \\ &= \sigma_2(a_{i1},\dots,a_{in_i})\theta^2 + \sigma_2\left(\frac{1}{a_{i1}},\dots,\frac{1}{a_{in_i}}\right)\theta^{-2} + \sum_{j=1}^{n_i}\left[\frac{-a_{ij}}{a_{ij}} + \frac{a_{ij}}{-a_{ij}}\right] \\ &= \sigma_2(a_{i1},\dots,a_{in_i})\theta^2 + \sigma_2\left(\frac{1}{a_{i1}},\dots,\frac{1}{a_{in_i}}\right)\theta^{-2} - 2n_i. \end{aligned} \tag{14}$$

Hence, if $\sigma_2(a_{i1},\dots,a_{in_i}) = \sigma_2(1/a_{i1},\dots,1/a_{in_i}) = 0$ for all $1 \le i \le r$, then the second-order leading coefficient of $g_d(y,1) - f(x) = \prod_{i=1}^{r} f_i(x,y)$ at y gives the contradiction

$$d = \sum_{i=1}^{r} 2n_i = 2\sum_{i=1}^{r} n_i = 2d. \tag{15}$$

So, $\sigma_2(a_{i1},\dots,a_{in_i})\sigma_2(1/a_{i1},\dots,1/a_{in_i}) \neq 0$ for some value i and consequently, using such particular value,

$$\theta^2 + c_i\theta^{-2} = \frac{h_{i2}(x) + 2n_i}{c_i} = H_{i2}(x) \in \bar{K}_q[x], \tag{16}$$

where $c_i = \sigma_2(1/a_{i1},\dots,1/a_{in_i})/\sigma_2(a_{i1},\dots,a_{in_i})$. Therefore,

$$\begin{gathered} g_d\left(\theta^2 + \frac{c_i}{\theta^2}, c_i\right) = \left(\frac{f(x) \pm \sqrt{f^2(x) - 4}}{2}\right)^2 + c_i^d\left(\frac{f(x) \mp \sqrt{f^2(x) - 4}}{2}\right)^2 = g_d(H_{i2}(x), c_i), \\ g_2(f(x), 1) = g_d(H_{i1}(x), c_i), \end{gathered} \tag{17}$$

where $c_i^d = 1$.

Since both cases contradict our assumptions on $f(x)$ and $g_2(f(x),1)$, then we conclude that $g_d(y,1) - f(x)$ is absolutely irreducible.

Corollary 4. *With conditions as in Theorem 3, let N denote the number of zeros of $g_d(y,1) - f(x)$ in $K_q \times K_q$. Let $e = \max\{d, \deg(f(x))\}$. Then,*

$$|N - q| \le (e-1)(e-2)\sqrt{q} + c(e) \tag{18}$$

for some constant $c(e)$.

Proof. Combine Theorem 3 and Weil's Riemann hypothesis theorem for curves over finite fields. ∎

References

[1] K. F. Ireland and M. I. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1998.
[2] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 65, Longman Scientific & Technical, Harlow, 1993.
[3] W. M. Schmidt, *Equations Over Finite Fields. An Elementary Approach*, Lecture Notes in Mathematics, vol. 536, Springer, Berlin, 1976.

Javier Gomez-Calderon: Department of Mathematics, The Pennsylvania State University, New Kensington Campus, New Kensington, PA 15068, USA
E-mail address: jxg11@psu.edu