ACTA ARITHMETICA
XC.4 (1999)

On Chebyshev polynomials and maximal curves

by

ARNALDO GARCIA (Rio de Janeiro, RJ) and
HENNING STICHTENOTH (Essen)

1. Introduction. The interest in curves (projective, nonsingular and geometrically irreducible) over finite fields with many rational points was renewed after Goppa's construction of codes from curves. Particularly interesting is the case of maximal curves over $K = \mathbb{F}_{q^2}$, i.e., curves C defined over K such that the number $\#C(K)$ of K-rational points attains the Hasse–Weil upper bound:

$$\#C(K) = q^2 + 1 + 2gq, \tag{1.1}$$

where $g = g(C)$ is the genus of the curve C.

Ihara [I] showed that the genus g of a maximal curve over K satisfies

$$g \le q(q-1)/2. \tag{1.2}$$

Rück and Stichtenoth [R-S] showed that there is a unique maximal curve over K with genus $g = q(q-1)/2$. Its associated function field is the so-called *Hermitian function field* H which is given by

$$H = K(x, y) \quad \text{with} \quad y^q + y = x^{q+1}. \tag{1.3}$$

In [G-S-X] we have determined the genera of several subfields of the Hermitian function field H (it is well known that they also correspond to maximal curves).

In order to have an explicit description of codes arising from curves one frequently needs that the curves (or their associated function fields) are explicitly given by equations. The subfields of H we are interested in here are among those appearing in [G-S-X, Theorem 5.4]. It will turn out that they can be described by using Chebyshev polynomials (see Remarks 4.4 and 5.2). Chebyshev polynomials are special cases of Dickson polynomials which have been intensively studied in connection with the theory of permutation polynomials over a finite field $\mathbb{F}_q$, the main result being that a Dickson

1991 *Mathematics Subject Classification*: 11C, 11R, 14H.

polynomial is a permutation polynomial over $\mathbb{F}_q$ if and only if its degree is relatively prime to q^2-1 (see [L-N, Theorem 7.16]). However, the Chebyshev polynomials that will be considered here have degrees dividing $q-1$.

The connection between Chebyshev polynomials and certain subfields of the Hermitian function field is explored here in both ways, i.e., we derive properties of these function fields from properties of Chebyshev polynomials (see Theorems 3.1 and 4.1) and conversely, we get properties of certain Chebyshev polynomials from the function fields considered (see Section 6). We also give alternate proofs for the genus formulas in [G-S-X, Example 5.5] (see Theorems 4.1 and 5.1).

2. Preliminaries. As before we denote by $K=\mathbb{F}_{q^2}$ the finite field with q^2 elements and by H the Hermitian function field given in (1.3). We will always assume that $\operatorname{char} K = p \neq 2$.

For a generator a of $K^\times = K\setminus\{0\}$ (i.e., a is a (q^2-1)th root of unity), let $\mathcal{C}$ be the group of automorphisms of H with $2(q^2-1)$ elements generated as below:

$$\mathcal{C} = \langle \varepsilon, \omega\rangle \quad \text{with } \varepsilon(x)=ax,\ \varepsilon(y)=a^{q+1}y \text{ and } \omega(x)=x/y,\ \omega(y)=1/y. \tag{2.1}$$

For a divisor m of q^2-1 we denote by $\mathcal{G}$ the subgroup of $\mathcal{C}$ with $2m$ elements given by

$$\mathcal{G} = \langle \lambda, \omega\rangle \quad \text{with} \quad \lambda = \varepsilon^{(q^2-1)/m}. \tag{2.2}$$

The subfields of the Hermitian function field we are interested in here are the fixed fields $H^{\mathcal{G}}$ under the automorphism group $\mathcal{G}$ in the following two cases:

Case 1: m is a divisor of $q-1$.
Case 2: m is a divisor of $q+1$.

It will turn out that in both cases the field $H^{\mathcal{G}}$ can be described by equations involving Chebyshev polynomials.

Definition 2.1. For a natural number $n\in\mathbb{N}$, the *nth Chebyshev polynomial* $\Phi_n(T)\in\mathbb{Z}[T]$ is the polynomial (monic of degree n) expressing X^n+X^{-n} in the variable $T=X+X^{-1}$, where X denotes a transcendental element over $\mathbb{Q}$.

3. Chebyshev polynomials. The relation between the polynomials defined above and the classical ones (i.e., the ones expressing $\cos n\theta$ as a polynomial in $\cos\theta$) is clear; just set $X=\exp(i\theta)$ (see [R]). We have $\Phi_1(T)=T$, $\Phi_2(T)=T^2-2$, $\Phi_3(T)=T^3-3T$ and $\Phi_4(T)=T^4-4T^2+2$. We have the following recursion formula:

$$\Phi_n(T) = T\Phi_{n-1}(T) - \Phi_{n-2}(T) \quad \text{for } n \ge 3. \tag{3.1}$$

From (3.1) it follows that

$$\Phi_n(T) = (T^2-2)\Phi_{n-2}(T) - \Phi_{n-4}(T) \quad \text{for } n \ge 5. \tag{3.2}$$

The polynomials which will play a role in the next sections are $\Phi_n(T)-2$ and $\Phi_n(T)+2$. From (3.2) one derives the following recursion formulas:

$$\begin{aligned}\Phi_n(T) - 2 \\ &= (T^2-2)(\Phi_{n-2}(T)-2) - (\Phi_{n-4}(T)-2) + 2(T-2)(T+2)\end{aligned} \tag{3.3}$$

and

$$\begin{aligned}\Phi_n(T) + 2 \\ &= (T^2-2)(\Phi_{n-2}(T)+2) - (\Phi_{n-4}(T)+2) - 2(T-2)(T+2).\end{aligned} \tag{3.4}$$

From (3.3) one sees that $T-2$ divides $\Phi_n(T)-2$ if n is odd, and T^2-4 divides $\Phi_n(T)-2$ if n is even.

From (3.4) one sees that $T+2$ divides $\Phi_n(T)+2$ if n is odd. Clearly, if n is even then $\Phi_n(T)+2$ is a square of a polynomial in T since

$$X^n + X^{-n} + 2 = (X^{n/2} + X^{-n/2})^2.$$

Our aim is to determine the quotient in all the cases above. It will turn out that these quotients are squares of polynomials in $\mathbb{Z}[T]$. To prove this we consider a much more general situation. For three polynomials $A(T)$, $P_0(T)$ and $P_1(T)$ with integer coefficients we define

$$\begin{aligned}\Psi_0(T) = A(T)P_0(T)^2, \quad \Psi_1(T) = A(T)P_1(T)^2, \\ F(T) = P_0(T)^2 + P_1(T)^2 - TP_0(T)P_1(T).\end{aligned}$$

For each $k \ge 1$ we define recursively

$$\Psi_{k+1}(T) = (T^2-2)\Psi_k(T) - \Psi_{k-1}(T) + 2A(T)F(T). \tag{3.5}$$

It then follows from (3.5) that $A(T)$ divides $\Psi_k(T)$ for all $k \ge 0$. The next theorem determines the quotient.

Theorem 3.1. *With notations as above we have*

$$\Psi_k(T) = A(T)P_k(T)^2,$$

where $P_k(T) \in \mathbb{Z}[T]$ is determined recursively by

$$P_{k+1}(T) = TP_k(T) - P_{k-1}(T) \quad \textit{for } k \ge 1. \tag{3.6}$$

Proof. Factoring out $A(T)$ in (3.5), we have to prove that the polynomials defined in (3.6) satisfy

$$P_{k+1}(T)^2 = (T^2-2)P_k(T)^2 - P_{k-1}(T)^2 + 2F(T). \tag{3.7}$$

Substituting (3.6) in (3.7), we need to show that for all $k \geq 1$,

$$TP_k(T)P_{k-1}(T) = P_{k-1}(T)^2 + P_k(T)^2 - F(T). \tag{3.8}$$

We will prove that (3.8) holds by induction on k, the case $k = 1$ following from the very definition of the polynomial $F(T)$. Now we want to prove that

$$TP_{k+1}(T)P_k(T) = P_k(T)^2 + P_{k+1}(T)^2 - F(T). \tag{3.9}$$

Again substituting (3.6) in (3.9), we need to prove that

$$TP_k(T)P_{k-1}(T) = P_{k-1}(T)^2 + P_k(T)^2 - F(T).$$

The theorem then follows from the induction hypothesis. ∎

Remark 3.2. For Chebyshev polynomials (shifted by ± 2) Theorem 3.1 applies with the following particular choices of the polynomials $A(T)$, $P_0(T)$ and $P_1(T)$.

Case $\Phi_n(T) - 2$: If $n = 2k + 1$ is an odd integer, we set $\Psi_k(T) = \Phi_{2k+1}(T) - 2$ and we choose $A(T) = T - 2$, $P_0(T) = 1$ and $P_1(T) = T + 1$. If $n = 2k + 2$ is an even integer, we set $\Psi_k(T) = \Phi_{2k+2}(T) - 2$ and we take $A(T) = T^2 - 4$, $P_0(T) = 1$ and $P_1(T) = T$.

Case $\Phi_n(T) + 2$: If $n = 2k + 1$ is an odd integer, we set $\Psi_k(T) = \Phi_{2k+1}(T) + 2$ and we choose $A(T) = T + 2$, $P_0(T) = 1$ and $P_1(T) = T - 1$. If $n = 2k + 2$ is an even integer, we set $\Psi_k(T) = \Phi_{2k+2}(T) + 2$ and we choose $A(T) = 1$, $P_0(T) = T$ and $P_1(T) = T^2 - 2$.

Of course, in all cases above one has to compute the corresponding function $F(T)$ and to show that (3.5) coincides with (3.3) or (3.4).

4. The case m divides $q - 1$. We denote $F = K(x^{q-1}, y^{q-1})$. Clearly, the extension $H|F$ is cyclic of degree $q-1$. For a divisor m of $q-1$ we denote by E_1 the unique intermediate field of $H|F$ satisfying $[H : E_1] = m$. The genus $g(E_1)$ of this intermediate field is given by (see [G-S-X, Corollary 4.9])

$$g(E_1) = \tfrac{1}{2}n(q + 1 - d), \tag{4.1}$$

where $n = (q - 1)/m$ and $d = \gcd(m, q + 1)$.

Since m is a divisor of $q - 1$, we have $d = 1$ if m is odd, and $d = 2$ if m is even.

We denote by E_1^ω the fixed subfield of E_1 under ω, where ω is the automorphism given in (2.1) (i.e., $E_1^\omega = H^{\mathcal{G}}$). The genus $g(E_1^\omega)$ is given by (see [G-S-X, Theorem 5.4])

$$g(E_1^\omega) = \tfrac{1}{4}n(q + 1 - d - m), \tag{4.2}$$

with notations as in (4.1).

Applying the Riemann–Hurwitz formula to the degree 2 extension $E_1|E_1^\omega$ and using (4.1) and (4.2), we conclude that there are exactly $q+1$ places that ramify in the extension $E_1|E_1^\omega$. The next theorem gives an alternate proof that exactly $q+1$ places ramify in $E_1|E_1^\omega$ (by describing them explicitly) and hence we also have an alternate proof of the genus formula in (4.2). This new approach will be based on the property of (shifted by two) Chebyshev polynomials given in Theorem 3.1 (see Remark 3.2).

THEOREM 4.1. *With notations as at the beginning of this section, there are exactly $q+1$ places of E_1^ω that ramify in the extension $E_1|E_1^\omega$. These places are the zeros in E_1^ω (each of them simple) of the function $y^m+y^{-m}-2$.*

Proof. For brevity we will prove the theorem only in the case where $n=(q-1)/m$ is an odd integer. We start with two lemmas (case $n=1$).

LEMMA 4.2. *Let $F=K(x^{q-1},y^{q-1})$ and let F^ω be its fixed subfield under the automorphism ω. Then F^ω is a rational function field and we have $F^\omega = K(x^2/y)$.*

Proof. It is easily verified that the function x^2/y is invariant under the group $\mathcal{G}$ described in (2.2) with $m=q-1$; i.e., we have $x^2/y \in F^\omega$. Computing the pole divisor of x^2/y in the Hermitian function field H, we get

$$\mathrm{div}_\infty(x^2/y) = (q-1)P_\infty + (q-1)P_0,$$

where P_∞ is the unique pole of x in H and P_0 is the unique common zero in H of the functions x and y.

Hence $[H : K(x^2/y)] = 2(q-1)$ and since $[H : F^\omega] = 2(q-1)$, the result follows. ■

The next lemma proves Theorem 4.1 for the case $m=q-1$ (i.e., for $n=1$).

LEMMA 4.3. *There are exactly $q+1$ places of F^ω that ramify in the extension $F|F^\omega$ and they are the zeros in F^ω (each of them simple) of the function $y^{q-1}+y^{-(q-1)}-2$.*

Proof. From (4.1) and Lemma 4.2, we have

$$g(F) = (q-1)/2 \quad \text{and} \quad g(F^\omega) = 0.$$

The assertion on the number of ramified places then follows from Hurwitz's formula for the extension $F|F^\omega$ (although we prove this assertion also below while describing the ramified places explicitly).

The extension $F^\omega|K(y^{q-1}+y^{-(q-1)})$ is a Kummer extension of degree $q+1$ with generator x^2/y satisfying

$$(x^2/y)^{q+1} = y^{q-1}+y^{-(q-1)}+2. \tag{4.3}$$

We set $t = y^{q-1}+y^{-(q-1)}$ and consider the degree 2 extension $K(y^{q-1})|K(t)$. It is easily seen that

$$(2y^{q-1} - t)^2 = (t+2)(t-2). \tag{4.4}$$

From (4.4) we see that ramification in the extension $K(y^{q-1})|K(t)$ occurs exactly at the zero of $t+2$ and at the zero of $t-2$. Now from (4.3) we see that the zero of $t+2$ is fully ramified in $F^\omega|K(t)$ and hence unramified in the extension $F|F^\omega$. Again from (4.3), the zero of $t-2$ is unramified in $F^\omega|K(t)$ and hence we have $q+1$ places of F^ω that are zeros of the function $t-2$ and all of them are simple. Clearly, these are the places of F^ω that ramify in $F|F^\omega$. ∎

We will use lower-case letters to denote reduction mod $p = \operatorname{char} K$; i.e., $\varphi_n(T)$ and $p_k(T) \in \mathbb{F}_p[T]$ are the reductions of $\Phi_n(T)$ and $P_k(T)$, respectively.

Now we return to the proof of Theorem 4.1. As already mentioned we will restrict ourselves to the case where $n = (q-1)/m$ is an odd integer. As before we denote by $\Phi_n(T)$ the Chebyshev polynomial of degree n. A generating equation for the extension $E_1^\omega|F^\omega$ of degree n is

$$\varphi_n(u) = y^{q-1} + y^{-(q-1)}, \quad \text{where} \quad u = y^m + y^{-m}. \tag{4.5}$$

From (4.5) and Remark 3.2, we get

$$y^{q-1} + y^{-(q-1)} - 2 = (u-2)p_k(u)^2 \quad \text{with} \quad k = (n-1)/2. \tag{4.6}$$

From Remark 3.2 and the recursion formula (3.6) one has $P_j(2) = 2j+1$ for all j. In particular for $k = (n-1)/2$ we have

$$P_k(2) = n \not\equiv 0 \pmod{p}.$$

This shows that $u = 2$ is a simple root of the right hand side in (4.6).

It follows from Lemma 4.3 that the places of E_1^ω that ramify in the extension $E_1|E_1^\omega$ are among the zeros of the function $y^{q-1} + y^{1-q} - 2$. The theorem now follows from equation (4.6).

Remark 4.4. As before we assume that n is odd. From (4.3) and (4.5) one sees that the field E_1^ω can be generated by two functions u and v satisfying the irreducible equation (i.e., the curve given below is a maximal curve having E_1^ω as its function field)

$$v^{q+1} = \varphi_n(u) + 2. \tag{4.7}$$

An explicit description of the field E_1 was already obtained in [G-S-X, Example 6.3].

5. The case m divides $q+1$. We denote here by E_2 the unique intermediate field of the extension $H|K(y)$ such that $[H : E_2] = m$, m being a divisor of $q+1$, and by E_2^ω the fixed subfield of E_2 under the automorphism

ω (i.e., $E_2^\omega = H^{\mathcal{G}}$). It is easily seen that $\mathcal{G}$ is an abelian group in this case. The extension $H^\omega|K(z)$, with $z = y + y^{-1}$, is a Kummer extension of degree $q+1$ having $x+\omega(x)$ as a Kummer generator. We have the following equations:

$$(x+\omega(x))^{q+1} = (y^{(q-1)/2} + y^{-(q-1)/2})(z+2)^{(q+1)/2} \tag{5.1}$$

and

$$(x+\omega(x))^{q+1} = (z+2) + (z+2)^q + (y^{q-1} + y^{-(q-1)} - 2). \tag{5.2}$$

Equation (5.1) follows from

$$(x+\omega(x))^{q+1} = \frac{x^{q+1}}{y^{(q+1)/2}}\left(\frac{(y+1)^2}{y}\right)^{(q+1)/2}$$

and (5.2) follows from

$$(x+\omega(x))^{q+1} = (y^q + y)(1 + y^{-1} + y^{-q} + y^{-(q+1)}).$$

We now consider the extension $K(y)|K(z)$ of degree 2. This extension is described by

$$(2y-z)^2 = (z+2)(z-2). \tag{5.3}$$

Equation (5.3) shows that the ramified places in the extension $K(y)|K(z)$ are exactly the zero of $z+2$ and the zero of $z-2$. The places of $K(y)$ above these two places are the zero of $y+1$ and the zero of $y-1$, respectively. From the generating equation of $H|K(y)$,

$$x^{q+1} = y + y^q,$$

we see that these two places of $K(y)$ are unramified in the extension $H|K(y)$.

The next theorem gives an alternate proof for the genus formula in [G-S-X, Example 5.5].

Theorem 5.1. *With notations as at the beginning of this section, we have*

$$g(E_2^\omega) = \begin{cases} (q-3)(q+1-m)/(4m) & \text{if } m \text{ is even}, \\ ((q-3)(q+1-m)+(q+1))/(4m) & \text{if } m \text{ is odd.} \end{cases}$$

Proof. We first determine some of the ramified places in the extension $E_2^\omega|K(z)$ of degree $(q+1)/m$. We have exactly $q+1$ places of $K(y)$ that are ramified in the extension $H|K(y)$ and all of them are fully ramified. Those places of $K(y)$ are the zero of y, the pole of y and the zero of $y-\alpha$, where $\alpha^{q-1} = -1$. This gives us $(q+1)/2$ fully ramified places in the extension $E_2^\omega|K(z)$, since we have the identification of the zero of y with the pole of y (both being the places of $K(y)$ above the pole of z) and also the identification of the zero of $y-\alpha$ with the zero of $y-\alpha^{-1}$ (both being the places of $K(y)$ above the zero of $z-(\alpha+\alpha^{-1})$). It follows from equation (5.1) that the zero of $z-2$ is unramified in $E_2^\omega|K(z)$. Apart from the $(q+1)/2$ fully ramified places mentioned before, the other possible ramification in the extension $E_2^\omega|K(z)$ must then occur over the zero of the function $z+2$ (see (5.3)). Again, from (5.1) we deduce the following Kummer equation for the extension $E_2^\omega|K(z)$:

$$[(x+\omega(x))^m]^{(q+1)/m} = (y^{(q-1)/2}+y^{-(q-1)/2})(z+2)^{(q+1)/2}.$$

From the theory of Kummer extensions [S, Prop. III.7.3] we then find that the ramification index e of the zero of $z+2$ in the extension $E_2^\omega|K(z)$ is given by

$$e = \frac{(q+1)/m}{\gcd((q+1)/m,(q+1)/2)} = \begin{cases} 1 & \text{if } m \text{ is even,}\\ 2 & \text{if } m \text{ is odd.}\end{cases}$$

Now the theorem follows from the Hurwitz genus formula applied to the extension $E_2^\omega|K(z)$. ■

We conclude this section with a remark describing the field E_2^ω explicitly.

Remark 5.2. From (5.2) we see that the field E_2^ω can be generated by two functions v and u satisfying the irreducible equation (i.e., the curve given below is a maximal curve having E_2^ω as its function field)

$$v^{(q+1)/m} = u+u^q+\varphi_{q-1}(u-2)-2,$$

where $\varphi_{q-1}(T)$ is the reduction modulo p of the Chebyshev polynomial.

An explicit description of the field E_2 was already obtained in [G-S-X, Example 6.3].

6. Properties of (reduced) Chebyshev polynomials. We will use here the function fields of Sections 4 and 5 to derive certain properties of the associated Chebyshev polynomials. We start with a separability property:

Theorem 6.1. *With notations as before, we have*:

(a) *If n is an odd divisor of $q-1$ then*

$$\varphi_n(T)+2 = (T+2)p(T)^2,$$

where $p(T)\in\mathbb{F}_p[T]$ is a separable polynomial of degree $(n-1)/2$ having all roots in $\mathbb{F}_{q^2}$ such that $p(-2)\neq 0$.

(b) *The polynomial $\varphi_{(q-1)/2}(T)$ is a separable polynomial having all roots in $\mathbb{F}_{q^2}$ such that $\varphi_{(q-1)/2}(-2)\neq 0$.*

Proof. (a) The polynomial $p(T)$ is just the polynomial $p_k(T)$ with $k=(n-1)/2$ obtained from the recursion formula (3.6) with the choice $P_0(T)=1$ and $P_1(T)=T-1$ (see Remark 3.2). From (3.6) and the choices of $P_0(T)$ and $P_1(T)$ above one deduces that

$$p_k(-2) = (-1)^k(2k+1) = (-1)^k n \neq 0.$$

Now we are going to show that $p(T)$ is indeed separable. Equation (4.7) shows that $E_1^\omega|K(u)$ is a Kummer extension of degree $q+1$ and the genus

$g(E_1^\omega)$ is given by (4.2) with $d = 2$, since m is even in our case. Computing also the genus of E_1^ω using [S, Prop. III.7.3], we conclude that $p_k(T)$ is a separable polynomial.

(b) From (5.1) we have the following equation for the maximal curve associated with field H^ω (notations as in Remark 5.2):

$$v^{q+1} = u^{(q+1)/2}\varphi_{(q-1)/2}(u-2).$$

From Theorem 5.1 with $m = 1$, we have $g(H^\omega) = (q-1)^2/4$. Again, computing also the genus of H^ω using [S, Prop. III.7.3], we get the desired result on the separability of $\varphi_{(q-1)/2}(T)$.

The assertions on the roots belonging to $\mathbb{F}_{q^2}$ follow since no place of degree 3 of H ramifies in the extensions considered (see [G-S-X]). They also follow from Sections 4 and 5 here. ■

For a polynomial $\varphi(T)$ we set

$$N(\varphi) = \#\{\alpha \in \mathbb{F}_{q^2} \mid \varphi(\alpha) \in \mathbb{F}_q\}.$$

Clearly we have $N(\varphi) \le q \deg \varphi(T)$. The next theorem determines $N(\varphi)$ for certain Chebyshev polynomials and it turns out that this number is about half the upper bound $q \deg \varphi(T)$.

THEOREM 6.2. *With notations as above, we have*:

(a) *If n is an odd divisor of $q-1$ then*

$$N(\varphi_n) = \frac{q(n+1)-(n-1)}{2}.$$

(b) *For the Chebyshev polynomial $\varphi_{q-1}(T)$ we have*

$$N(\varphi_{q-1}) = (q^2+1)/2.$$

Proof. (a) Equation (4.7) is the equation of a maximal curve over K whose function field is E_1^ω. Its number $N(K)$ of rational points over K is given by

$$N(K) = q^2 + 1 + 2\cdot\tfrac{1}{4}n(q-1-m)q.$$

Using Theorem 6.1(a) and (4.7) one sees that the number of ramified places in the extension $E_1^\omega|K(u)$ is exactly $n+1$. Simple computations give

$$\frac{N(K)-(n+1)}{q+1} = \frac{qn+q-2n}{2}.$$

Since all the $k+1$ zeros of $\varphi_n(T)+2$ belong to K, we have

$$N(\varphi_n) = \frac{qn+q-2n}{2} + k + 1 = \frac{q(n+1)-(n-1)}{2}.$$

(b) The proof here is similar to the one in part (a) above, using the fact that the field H^ω has genus $(q-1)^2/4$ and that it can be given by (notations as in Remark 5.2)

$$v^{q+1} = u + u^q + \varphi_{q-1}(u-2) - 2.$$

Notice that $\alpha + \alpha^q$ has values in $\mathbb{F}_q$ for $\alpha \in \mathbb{F}_{q^2}$. ■

REMARK 6.3. For an odd divisor n of $q-1$ or for $n = q-1$, we consider the curve given by

$$v^q + v = \varphi_n(u).$$

Its genus g and its number N of K-rational points (which is roughly half of Weil's upper bound) are

$$g = \frac{(q-1)(n-1)}{2} \quad \text{and} \quad N = 1 + qN(\varphi_n),$$

where $N(\varphi_n)$ is given in Theorem 6.2.

THEOREM 6.4. *Let p be an odd prime number and q be a power of p. Then the polynomial*

$$\Phi_{q-1}(T-2) \in \mathbb{Z}[T]$$

is such that all coefficients of the monomials T^j, with $1 < j < (q+1)/2$, are multiples of the prime number p.

Proof. From (5.1) and (5.2) we get

$$(y^{(q-1)/2} + y^{-(q-1)/2})(z+2)^{(q+1)/2} = (z+2) + (z+2)^q + (y^{q-1} + y^{-(q-1)} - 2).$$

Equivalently (with the notations of Remark 5.2) we have

$$(y^{(q-1)/2} + y^{-(q-1)/2})u^{(q+1)/2} = u + u^q + \varphi_{q-1}(u-2) - 2.$$

Hence $\varphi_{q-1}(u-2)$ as a polynomial in u has the form

$$\varphi_{q-1}(u-2) = 2 - u + (-1)^{(q-1)/2} 2u^{(q+1)/2} + \ldots,$$

where the dots stand for higher degree terms.

This finishes the proof of the theorem. ■

REMARK 6.5. Using the explicit description of Dickson polynomials given in [L-N, (7.6), p. 355], one can write the assertion of Theorem 6.4 purely in terms of binomial coefficients.

References

[G-S-X] A. Garcia, H. Stichtenoth and C. P. Xing, *On subfields of the Hermitian function field*, Compositio Math., to appear.

[I] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo 28 (1981), 721–724.

[L-N] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, Reading, MA, 1983.

[R] T. J. Rivlin, *Chebyshev Polynomials*, Wiley, New York, 1990.

[R-S] H. G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. 457 (1994), 185–188.

[S] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

Instituto de Matématica Pura e Aplicada IMPA
22460-320 Rio de Janeiro, RJ
Brazil
E-mail: garcia@impa.br

Universität GH Essen
FB 6
Mathematik u. Informatik
45117 Essen, Germany
E-mail: stichtenoth@uni-essen.de

Received on 10.6.1998
and in revised form on 1.4.1999 (3401)