AN EXTREMAL PROPERTY OF FEKETE POLYNOMIALS

PETER BORWEIN, KWOK-KWONG STEPHEN CHOI AND SOROOSH YAZDANI

ABSTRACT. The Fekete polynomials are defined as

$$F_q(z) := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k$$

where $\left(\frac{\cdot}{q}\right)$ is the Legendre symbol. These polynomials arise in a number of contexts in analysis and number theory. For example, after cyclic permutation they provide sequences with smallest known L_4 norm out of the polynomials with ± 1 coefficients.

The main purpose of this paper is to prove the following extremal property that characterizes the Fekete polynomials by their size at roots of unity.

Theorem 0.1. *Let $f(x) = a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$ with odd N and $a_n = \pm 1$. If*

$$\max\{|f(\omega^k)| : 0 \le k \le N-1\} = \sqrt{N},$$

then N must be an odd prime and $f(x)$ is $\pm F_q(x)$. Here $\omega := e^{\frac{2\pi i}{N}}$.

This result also gives a partial answer to a problem of Harvey Cohn on character sums.

Date: October 18, 1999.

1991 *Mathematics Subject Classification.* 11J54, 11B83, 12-04 .

Key words and phrases. Class Number; $-1, 1$ coefficients; Merit factor; Fekete polynomials; Turyn Polynomials; Littlewood polynomials.

Research of P. Borwein is supported, in part, by NSERC of Canada. K.K. Choi is a Pacific Institute of Mathematics Postdoctoral Fellow and the Institute's support is gratefully acknowledged.

1. Introduction

As in the abstract the Fekete polynomials are defined as

$$F_q(z) := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k$$

where $\left(\frac{\cdot}{q}\right)$ is the Legendre symbol. In [4] we gave explicit formulas for the L_4 norm (or equivalently for the merit factors) of various sequences of polynomials related to the Fekete polynomials. For example for q an odd prime,

$$\|F_q\|_4^4 := \frac{5q^2}{3} - 3q + \frac{4}{3} - 12(h(-q))^2$$

where $h(-q)$ is the class number of $\mathbb{Q}(\sqrt{-q})$. A similar explicit formula is given for an example of Turyn's that is constructed by cyclically permuting the first quarter of the coefficients of F_q. This is the sequence of polynomials with ± 1 coefficients that has the smallest known asymptotic L_4 norm on the unit disc (see [4] where this old problem is discussed further). Explicitly,

$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k + [q/4]}{q}\right) z^k$$

where $[\cdot]$ denotes the nearest integer, satisfies

$$\|R_q\|_4^4 = \frac{7q^2}{6} - q - \frac{1}{6} - \gamma_q$$

where

$$\gamma_q := \begin{cases} h(-q)(h(-q)-4) & \text{if} \quad q \equiv 1, 5 \pmod 8, \\ 12(h(-q))^2 & \text{if} \quad q \equiv 3 \pmod 8, \\ 0 & \text{if} \quad q \equiv 7 \pmod 8). \end{cases}$$

The point of this note is to explore the sense in which the Fekete polynomials are extremal in the supremum norm on the disc. Because of Gauss' lemma, we have for $0 \le k \le q-1$

$$F_q(e^{\frac{2\pi i k}{q}}) = \begin{cases} \sqrt{q}\left(\frac{k}{q}\right) & \text{if } q \equiv 1 \pmod 4, \\ i\sqrt{q}\left(\frac{k}{q}\right) & \text{if } q \equiv 3 \pmod 4). \end{cases}$$

and we see that F_q is of constant modulus on the qth roots of unity. The point of this note is to prove that F_q is also uniquely of smallest possible supremum norm at these points. Precisely

Theorem 1.1. *Let $f(x) = a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$ with odd N and $a_n = \pm 1$. Then we have*

$$\sum_{k=0}^{N-1} |f(\omega^k)|^4 \ge N^2(N-1) \tag{1.1}$$

and

$$\max\{|f(\omega^k)| : 0 \le k \le N-1\} \ge \sqrt{N}. \tag{1.2}$$

Inequalities (1.1) *and* (1.2) *are optimal and equality holds in* (1.2) *if and only if N is an odd prime and $f(x)$ is $\pm F_q(x)$. Here $\omega := e^{\frac{2\pi i}{N}}$.*

We should remark here that Theorem 1.1 is not really restricted to polynomials with zero constant term since multiplication by x does not change the value of $|f(\omega^k)|$. The assumption that $a_0 = 0$ in Theorem 1.1 just simplifies the presentation.

Despite the fact that Fekete polynomial F_q has modulus $\sqrt{q}$ at each qth root of unity Montgomery ([8]) shows that the supremum norm on the whole unit disc grows at least like $\sqrt{q}\log\log q$. This and further properties of Fekete polynomials, including, the behavior of their zeros are discussed in [6].

A consequence of Theorem 1.1 is the following. If $f(x)$ is a polynomial in Theorem 1.1 with $a_0 = 0$, then from Lemma 3.1 below, the equality of (1.2) holds if and only if

$$|f(\omega^k)|^2 = \begin{cases} 0 & \text{if } k = 0, \\ N & \text{if } k \neq 0, \end{cases}$$

which can also be shown (see Theorem 3 in [7]) to be equivalent to

$$\sum_{n=0}^{N-1} a_n a_{n+k} = \begin{cases} N-1 & \text{if } k = 0, \\ -1 & \text{if } k \neq 0. \end{cases}$$

It follows from Theorem 1.1 that

Corollary 1.2. *If $\psi : \mathbb{Z}_N \longrightarrow \mathbb{R}$ is a mapping such that $\psi(0) = 0, \psi(1) = 1, |\psi(a)| = 1$ for all $a \neq 0$ in $\mathbb{Z}_N$, then*

$$\sum_{n=0}^{N-1} \psi(n)\psi(n+k) = -1 \quad \textit{for all } k \neq 0$$

if and only if $N = q$ and ψ is the Legendre symbol modulo q.

This corollary gives a partial answer to a problem of Harvey Cohn on character sums. He asks (see p.202 in [9]) whether a multiplicative character can be characterized by a kind of "two-level autocorrelation" property, viz.

> If F is a finite field, $\psi : F \longrightarrow \mathbb{C}$ with $\psi(0) = 0, \psi(1) = 1, |\psi(a)| = 1$ for all $a \neq 0$ in F, and $\sum_{b \in F} \psi(b)\overline{\psi(b+a)} = -1$ for all $a \neq 0$, does it follow that ψ is a nontrivial multiplicative character of F?

Corollary 1.2 shows that for the case $\psi : \mathbb{F}_q \longrightarrow \mathbb{R}$, the answer to Cohn's problem is affirmative. The same result is also proved independently by S-L. Ma, M-K. Siu and Z. Zheng in [7] and A. Biró in [3]. Recently, M-K. Siu and the second author have solved Cohn's problem and they showed in [5] that the answer to Cohn's problem is negative when $|F| = q^s > 4$ and $s > 1$. They in fact gave many counter-examples for non-multiplicative functions which satisfy the two-level autocorrelation property. The idea of their proof originates from our Theorem 1.1.

2. Results

Let $f(x) = a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$ with odd N and $a_n = \pm 1$. Let $D^* := \{1 \leq n \leq N-1 : a_n = 1\}$ and $D := D^* \cup \{0\}$. For any $1 \leq n \leq N-1$, we define $b_n := \frac{a_n+1}{2}$ and hence

$$b_n = \begin{cases} 1 & \text{if } n \in D^*, \\ 0 & \text{otherwise}. \end{cases} \tag{2.1}$$

We denote $e^{\frac{2\pi i}{N}}$ by ω. Since $a_n = \pm 1$, we have

$$\sum_{k=0}^{N-1} |f(\omega^k)|^2 = \sum_{n,m=1}^{N-1} a_n a_m \sum_{k=0}^{N-1} \omega^{k(n-m)} = N(N-1). \tag{2.2}$$

On the other hand,

$$\begin{aligned}
\sum_{k=0}^{N-1} |f(\omega^k)|^4 &= \sum_{k=0}^{N-1} |f(\omega^k) f(\omega^{-k})|^2 \\
&= \sum_{k=0}^{N-1} \left| \sum_{l=0}^{N-1} \left\{ \sum_{n-m\equiv l \pmod N}^{N-1} a_n a_m \right\} \omega^{kl} \right|^2 \\
&= N \sum_{l=0}^{N-1} \left\{ \sum_{n-m\equiv l \pmod N}^{N-1} a_n a_m \right\}^2 \\
&= N \left\{ (N-1)^2 + \sum_{l=1}^{N-1} \left\{ \sum_{n-m\equiv l \pmod N}^{N-1} a_n a_m \right\}^2 \right\} \\
&\geq N((N-1)^2 + (N-1)) = N^2(N-1) \qquad (2.3)
\end{aligned}$$

because

$$\sum_{n-m\equiv l \pmod N}^{N-1} a_n a_m \equiv N-2 \equiv 1 \pmod 2$$

for $1 \leq l \leq N-1$. Thus we have the following lemma

Lemma 2.1. *Let $f(x) = a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$ with odd N and $a_n = \pm 1$. We have*

$$\sum_{k=0}^{N-1} |f(\omega^k)|^2 = N(N-1)$$

and

$$\sum_{k=0}^{N-1} |f(\omega^k)|^4 \geq N^2(N-1). \tag{2.4}$$

Furthermore, we have

$$\sum_{0\leq i<j\leq N-1} \left(N - |f(\omega^i)|^2\right)\left(N - |f(\omega^j)|^2\right) \leq 0. \tag{2.5}$$

Proof. It remains to prove (2.5). If we let $x_i = N - |f(\omega^i)|^2$ for $0 \leq i \leq N-1$, then (2.2) and (2.3) become

$$\sum_{i=0}^{N-1} x_i = N \tag{2.6}$$

and

$$\sum_{i=0}^{N-1} x_i^2 \geq N^2. \tag{2.7}$$

Now taking the square of both sides in (2.6) and using (2.7), we get

$$N^2 = \sum_{i=0}^{N-1} x_i^2 + 2 \sum_{0 \leq i < j \leq N-1} x_i x_j \geq N^2 + 2 \sum_{0 \leq i < j \leq N-1} x_i x_j.$$

This proves (2.5). It should also be noted that from (2.3), the equality of (2.4) holds if and only if $\sum_{n-m\equiv l \pmod N}^{N-1} a_n a_m = \pm 1$ for $1 \leq l \leq N-1$. □

Now inequality (1.2) is an immediate consequence of (2.5). For if $|f(\omega^k)|^2 < N$, then the summation in (2.5) would be positive and this contradicts (2.5).

By Gauss's lemma (see §9.10 in [1]), we have for $0 \leq k \leq q-1$

$$F_q(e^{\frac{2\pi i k}{q}}) = \begin{cases} \sqrt{q}\left(\frac{k}{q}\right) & \text{if } q \equiv 1 \pmod 4, \\ i\sqrt{q}\left(\frac{k}{q}\right) & \text{if } q \equiv 3 \pmod 4. \end{cases} \tag{2.8}$$

This shows that the inequality (1.2) is actually optimal and the equality can be attained by Fekete polynomials. We are going to prove Theorem 1.1 and this shows that Fekete polynomials are the only polynomials attaining the equality of (1.2).

3. Proof of Theorem 1.1

Lemma 3.1. *Let $f(x) = a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$ with odd N and $a_n = \pm 1$. If the equality of (1.2) holds, then*

$$|f(\omega^k)|^2 = N \tag{3.1}$$

for $1 \leq k \leq N-1$ and $f(1) = 0$.

Proof. If the equality of (1.2) holds, then $(N - |f(\omega^i)|^2) \geq 0$ for all i and hence

$$0 \leq \sum_{0 \leq i < j \leq N-1} (N - |f(\omega^i)|^2)(N - |f(\omega^j)|^2).$$

Now from (2.5), the above double summation must be zero and hence every term $(N - |f(\omega^i)|^2)(N - |f(\omega^j)|^2)$ must also be zero for $0 \leq i \neq j \leq N-1$ since they are all non-negative. On the other hand, since $|f(\omega^j)| = |f(\omega^{N-j})|$, if $1 \leq j \leq N-1$, then $j \neq N-j$ and

$$0 = (N - |f(\omega^j)|^2)(N - |f(\omega^{N-j})|^2) = (N - |f(\omega^j)|^2)^2.$$

It follows that $|f(\omega^j)|^2 = N$ for all $1 \leq j \leq N-1$. Finally, $f(1) = 0$ follows from (2.2). □

Lemma 3.2. *Let $f(x) = a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$ with odd N and $a_n = \pm 1$. If the equality of (1.2) holds, then $f(x)$ is symmetric if $N \equiv 1 \pmod 4$ and is anti-symmetric if $N \equiv 3 \pmod 4$.*

Proof. Let $g(x) = f(x) + 1 + x + \cdots + x^{N-1}$. On using (2.1)

$$g(x) = 1 + 2 \sum_{n=1}^{N-1} b_n x^n.$$

Also from Lemma 3.1, we have $g(1) = N$ and $|g(\omega^k)|^2 = |f(\omega^k)|^2 = N$ for $1 \le k \le N-1$. It follows that

$$g(x)g(x^{-1}) \equiv N + (N-1)\frac{x^N - 1}{x-1} \pmod{x^N - 1} \tag{3.2}$$

by evaluating both sides at 1 and the N-th roots of unity. On the other hand,

$$\begin{aligned} g(x)g(x^{-1}) &\equiv \left(1 + 2\sum_{k=1}^{N-1} b_k x^k\right)\left(1 + 2\sum_{k=1}^{N-1} b_k x^{N-k}\right) \\ &\equiv 1 + 2\sum_{k=1}^{N-1}(b_k + b_{N-k})x^k + 4\sum_{k=0}^{N-1}\theta_k x^k \\ &\equiv 2N - 1 + \sum_{k=1}^{N-1}\left(4\theta_k + 2b_k + 2b_{N-k}\right)x^k \pmod{x^N - 1}. \qquad (3.3) \end{aligned}$$

Here

$$\theta_k = \sum_{i-j \equiv k \pmod{N}} b_i b_j$$

for $0 \le k \le N-1$ and we have used that $|D^*| = \frac{N-1}{2}$ because $f(1) = 0$. Comparing coefficients in (3.2) and (3.3), we have

$$4\theta_k + 2b_k + 2b_{N-k} = N - 1 \tag{3.4}$$

for $1 \le k \le N-1$. Hence $2(b_k + b_{N-k}) \equiv N - 1 \pmod 4$ for $1 \le k \le N-1$. Therefore if $N \equiv 1 \pmod 4$, we have

$$b_k + b_{N-k} \equiv 0 \pmod 2$$

and hence $b_k = b_{N-k}$ for $1 \le k \le N-1$ because b_k is either 0 or 1. So $f(x)$ is symmetric. Similarly, if $N \equiv 3 \pmod 4$, we have

$$b_k + b_{N-k} \equiv 1 \pmod 2$$

and hence b_k and b_{N-k} are different for $1 \le k \le N-1$. So $f(x)$ is anti-symmetric. This proves Lemma 3.2. □

Let $\Phi_l(x)$ be the lth cyclotomic polynomial.

Lemma 3.3. *Let $G(x)$ be a polynomial of degree $N-1$ with integer coefficients and for any divisor d of N, let*

$$G_d(x) \equiv G(x) \pmod{\Phi_d(x)}.$$

Then

$$G(x) \equiv \frac{1}{N}\sum_{d|N} G_d(x)B_d(x) \pmod{x^N - 1}$$

where

$$B_d(x) := \sum_{r|d} \mu(d/r) r \frac{x^N - 1}{x^r - 1}$$

and $\mu(r)$ is Möbius function.

Proof. By the Chinese Remainder Theorem, we only need to verify that

$$\frac{1}{N}\sum_{d|N} G_d(x)B_d(x) \equiv G_r(x) \pmod{\Phi_r(x)}$$

for all divisors r of N. Clearly, if r and s are divisors of N, then

$$\frac{x^N-1}{x^s-1} \equiv \begin{cases} \frac{N}{s} \pmod{\Phi_r(x)} & \text{if } r \text{ divides } s, \\ 0 \pmod{\Phi_r(x)} & \text{otherwise.} \end{cases}$$

Thus when d divides N, we have

$$B_d(x) \equiv \sum_{r|s,s|d} \mu\left(\frac{d}{s}\right) s\frac{N}{s} \equiv N \sum_{r|s,s|d} \mu\left(\frac{d}{s}\right) \pmod{\Phi_r(x)}.$$

It follows that $B_d(x) \equiv N \pmod{\Phi_d(x)}$ and $B_d(x) \equiv 0 \pmod{\Phi_r(x)}$ if $r \neq d$. This proves our lemma. □

We now come to the proof of Theorem 1.1. If $N \equiv 3 \pmod 4$, then since $f(x)$ is anti-symmetric, $f(\omega^k)$ is purely imaginary for $1 \le k \le N-1$. Hence if we let $F(x) = 1 + f(x)$, then

$$|F(\omega^k)|^2 = |1 + f(\omega^k)|^2 = 1 + |f(\omega^k)|^2 = N+1.$$

for $1 \le k \le N-1$ and $F(1) = 1$. Recall that $D^* = \{1 \le n \le N-1 : a_n = 1\}$ and $D = D^* \cup \{0\}$ where $f(x) = \sum_{n=1}^{N-1} a_n x^n$. It turns out that D is a cyclic difference set. A subset $E = \{d_1, d_2, \cdots, d_k\}$ of $\mathbb{Z}_N$ is a (cyclic) (N,k,λ)-difference set (see [2]) if for any $\alpha \not\equiv 0 \pmod N$ the congruence equation $d_i - d_j \equiv \alpha \pmod N$ has exactly λ solution pairs (d_i, d_j) in $E \times E$. If we let

$$e_n = \begin{cases} 1 & \text{if } n \in E, \\ -1 & \text{if } n \notin E, \end{cases}$$

it is known (see §1.D in [2]) that E is a (N,k,λ)-difference set if and only if

$$\sum_{n-m\equiv k \pmod N}^{N-1} e_n e_m = \begin{cases} N & \text{if } k \equiv 0 \pmod N, \\ N - 4(k-\lambda) & \text{otherwise.} \end{cases} \tag{3.5}$$

Johnsen proved (see Theorem 4.15 of [2]) that the only cyclic difference sets with parameters $N = 4t-1, k = 2t-1$ and $\lambda = t-1$ for some positive integer t and $e_n = -e_{N-n}$ for $1 \le n \le N-1$ are given by the quadratic residues of a prime $\equiv 3 \pmod 4$, more precisely, N must be an odd prime $\equiv 3 \pmod 4$ and $e_n = e_0\left(\frac{n}{N}\right)$ for $1 \le n \le N-1$. Using similar calculation as in the proof of (2.3), one can show that if $|F(\omega^k)|^2 = N+1$ for all $1 \le k \le N-1$, then condition (3.5) is satisfied with $k = \frac{N-1}{2}$ and $\lambda = \frac{N+1}{4}$. Thus D is a cyclic $(N, \frac{N-1}{2}, \frac{N-3}{4})$-difference set. For $N \equiv 3 \pmod 4$, D satisfies the conditions in Johnsen's theorem since $f(x)$ is anti-symmetric. Hence $N = q$ and $f(x) = \pm F_q(x)$ by Johnsen's theorem. For the case $N \equiv 1 \pmod 4$, D is no longer a cyclic difference set. However, using similar methods to the proof of Johnsen's Theorem, we can still conclude that $f(x) = \pm F_q(x)$. Since $f(x)$ is symmetric in this case, $f(\omega^k)$ is real and hence $f(\omega^k) = \pm\sqrt{N}$ for $1 \le k \le N-1$. For any divisor $d > 1$ of N, we let

$$f(e^{\frac{2\pi i}{d}}) = \epsilon_d \sqrt{N}, \tag{3.6}$$

where $\epsilon_d = \pm 1$. We first claim that N can't be a perfect square. Suppose not, then $\sqrt{N}$ is an integer. So from (3.6)

$$f(x) \equiv \epsilon_d \sqrt{N} \pmod{\Phi_d(x)}$$

for any divisor $d > 1$ of N and $f(x) \equiv 0 \pmod{\Phi_1(x)}$ because $f(1) = 0$. By Lemma 3.3, we have

$$\begin{aligned} f(x) &\equiv \frac{1}{N} \sum_{d|N, d>1} \epsilon_d \sqrt{N} B_d(x) \\ &\equiv \frac{1}{\sqrt{N}} \sum_{d|N, d>1} \epsilon_d \sum_{r|d} \mu\left(\frac{d}{r}\right) r \frac{x^N - 1}{x^r - 1} \pmod{x^N - 1}. \end{aligned}$$

Considering the absolute value of the coefficient of the term x at both sides which only comes from the term when $r = 1$ on the right hand side, we have

$$1 = \left| \frac{1}{\sqrt{N}} \sum_{d|N, d>1} \epsilon_d \mu(d) \right| \leq \frac{d(N) - 1}{\sqrt{N}}$$

where $d(N)$ is the number of divisors of N. However, $d(N) \leq \sqrt{N}$ when N is odd. This is a contradiction. Thus N can't be a perfect square and hence $\sqrt{N} \notin \mathbb{Q}$. Next we suppose p and q are two distinct primes dividing N, then $f(e^{\frac{2\pi i}{p}}) = \epsilon_p \sqrt{N}$ belongs to $\mathbb{Q}(e^{\frac{2\pi i}{p}})$ and $f(e^{\frac{2\pi i}{q}}) = \epsilon_q \sqrt{N}$ belongs to $\mathbb{Q}(e^{\frac{2\pi i}{q}})$. So $\sqrt{N}$ belongs to $\mathbb{Q}(e^{\frac{2\pi i}{p}}) \cap \mathbb{Q}(e^{\frac{2\pi i}{q}}) = \mathbb{Q}$. This contradicts that $\sqrt{N} \notin \mathbb{Q}$ and therefore, N must be a prime power. Now let $N = q^s$ with odd s. Without loss of generality, we assume that $\epsilon_q = 1$. If $s = 1$, then from (2.8), we have

$$f(\omega) = F_q(\omega)$$

and hence $f(\omega^k) = F_q(\omega^k)$ for $0 \leq k \leq q-1$ by considering their images under the automorphisms of $\mathbb{Q}(\omega)$ which map ω to ω^k for $1 \leq k \leq q-1$. Since they have the same degree less than q, $f(x)$ must be $F_q(x)$. It remains to show that s can't be greater than 1. From (2.8), we have

$$f(e^{\frac{2\pi i}{q^j}}) = \epsilon_{q^j} q^{\frac{s-1}{2}} F_q(e^{\frac{2\pi i}{q}})$$

for $j = 1, 2, \cdots, s$. Hence

$$f(x) \equiv \epsilon_{q^j} q^{\frac{s-1}{2}} F_q(x^{q^{j-1}}) \pmod{\Phi_{q^j}(x)}$$

for $j = 1, 2, \cdots, s$ and $f(x) \equiv 0 \pmod{\Phi_1(x)}$. By Lemma 3.3, we have

$$f(x) \equiv \frac{1}{N} \sum_{j=1}^{s} \epsilon_{q^j} q^{\frac{s-1}{2}} F_q(x^{q^{j-1}}) B_{q^j}(x) \pmod{x^N - 1}. \tag{3.7}$$

Since $\mu(1) = 1, \mu(q) = -1$ and $\mu(q^j) = 0$ if $j \geq 2$, (3.7) becomes

$$\begin{aligned} f(x) \equiv{}& \epsilon_{q^s} q^{\frac{s-1}{2}} F_q(x^{q^{s-1}}) - \frac{1}{N} \epsilon_q q^{\frac{s-1}{2}} F_q(x) \frac{x^N - 1}{x - 1} + \\ & \frac{1}{N} \sum_{j=1}^{s-1} q^{\frac{2j+s-1}{2}} \left(\frac{x^N - 1}{x^{q^j} - 1}\right) \left\{ \epsilon_{q^j} F_q(x^{q^{j-1}}) - \epsilon_{q^{j+1}} F_q(x^{q^j}) \right\} \pmod{x^N - 1}. \end{aligned} \tag{3.8}$$

Since $F_q(1) = 0$,

$$F_q(x^{q^j})\frac{x^N - 1}{x^{q^j} - 1} \equiv 0 \pmod{x^N - 1},$$

for $j = 0, 1, \cdots, s$. Thus, (3.8) becomes

(3.9)

$$f(x) \equiv \epsilon_{q^s} q^{\frac{s-1}{2}} F_q(x^{q^{s-1}}) + \frac{1}{N}\sum_{j=1}^{s-1} \epsilon_{q^j} q^{\frac{2j+s-1}{2}} F_q(x^{q^{j-1}})\frac{x^N - 1}{x^{q^j} - 1} \pmod{x^N - 1}.$$

Note that the degree of the polynomials $F_q(x^{q^{j-1}})\frac{x^N-1}{x^{q^j}-1}$ is less than N. So the polynomial in the right hand side of (3.9) must have integer coefficients. However, if $s \geq 3$, the coefficient of the term x, which only comes from the term $j = 1$, is equals to $\frac{1}{N}\epsilon_q q^{\frac{s+1}{2}} = q^{\frac{-s+1}{2}} \notin \mathbb{Z}$. Therefore s must be one and this completes the proof of Theorem 1.1

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, Berlin, 1980.
[2] L. D. Baumert, *Cyclic Difference Sets*, LNM **182**, Springer-Verlag, Berlin, 1971.
[3] A. Biró, *Notes on a Problem of H. Cohn*, J. Number Theory, to appear.
[4] P. Borwein and K-K. Choi, *Explicit Merit Factor Formulae For Fekete and Turyn Polynomials*, (in press).
[5] K-K. Choi and M-K Siu, *Counter-Examples to a Problem of Cohn on Classifying Characters*, (in press).
[6] B. Conrey, A.Granville and B.Poonen, *Zeros of Fekete Polynomials*, (in press).
[7] S-L Ma, M-K Siu and Z Zheng, *On a Problem of Cohn on Character Sums*, (in press).
[8] H.L. Montgomery, *An Exponential Sum Formed with the Legendre Symbol*, Acta Arith, **37** (1980), 375–380
[9] H.L. Montgomery, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS, No 84, AMS, 1994.

Department of Mathematics and Statistics, Simon Fraser University, Burnaby, British Columbia, Canada V5A 1S6, email: pborwein@math.sfu.ca

Department of Mathematics, The University of Hong Kong, Pokfulam Road, Hong Kong, SAR, CHINA, email: choi@maths.hku.hk

Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1, email: syazdani@undergrad.math.uwaterloo.ca