Equations in finite fields with restricted solution sets, I. (Character sums.)

Katalin Gyarmati, András Sárközy*

Abstract

In earlier papers, for "large" (but otherwise unspecified) subsets $\mathcal{A}$, $\mathcal{B}$ of $\mathbb{Z}_p$ and for $h(x) \in \mathbb{Z}_p[x]$, Gyarmati studied the solvability of the equations

$$a + b = h(x),$$

resp.

$$ab = h(x)$$

with $a \in \mathcal{A}$, $b \in \mathcal{B}$, $x \in \mathbb{Z}_p$, and for large subsets $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$ of $\mathbb{Z}_p$ Sárközy showed the solvability of the equations

$$a + b = cd,$$

resp.

$$ab + 1 = cd$$

with $a \in \mathcal{A}$, $b \in \mathcal{B}$, $c \in \mathcal{C}$, $d \in \mathcal{D}$. In this series of papers equations of this type will be studied in finite fields. In particular, in Part I of the series we will prove the necessary character sum estimates of independent interest some of which generalize earlier results.

2000 Mathematics Subject Classification: 11T24.

Key words and phrases: finite field, equation, character sum.

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. T043623, T043631 and T049693

1 Introduction

In [4] Gyarmati showed that if p is a prime, $h(x) \in \mathbb{Z}_p[x]$, $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$, and $|\mathcal{A}|, |\mathcal{B}|$ are "large" enough in terms of the degree of $h(x)$, more precisely,

$$|\mathcal{A}|\,|\mathcal{B}| > Cp$$

where C is a constant depending on the degree of $h(x)$, then there are $a \in \mathcal{A}$, $b \in \mathcal{B}$, $x \in \mathbb{Z}_p$ with

$$a + b = h(x), \tag{1.1}$$

resp.

$$ab = h(x). \tag{1.2}$$

(She also studied some further problems of similar flavor.)

In [6] and [7] Sárközy proved that if p is a prime and $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$ are "large" subsets of $\mathbb{Z}_p$, then the equations

$$a + b = cd, \tag{1.3}$$

resp.

$$ab + 1 = cd \tag{1.4}$$

can be solved with $a \in \mathcal{A}$, $b \in \mathcal{B}$, $c \in \mathcal{C}$, $d \in \mathcal{D}$; more precisely, if $|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| > p^3$, then (1.3) can be solved, and $|\mathcal{A}|\,|\mathcal{B}|\,|\mathcal{C}|\,|\mathcal{D}| > 100p^3$ is needed to ensure the solvability of (1.4).

The common feature of these results is that given an equation

$$f(a_1, \ldots, a_k, \ldots, a_n) = 0,$$

we are looking for solutions $a_1, \ldots, a_k, \ldots, a_n$ such that some of the a_i's, say, $a_1, \ldots, a_k$ are restricted to elements of "large" (but otherwise unspecified) subsets $\mathcal{A}_1, \ldots, \mathcal{A}_k$ of $\mathbb{Z}_p$. In this series our goal is to generalize these results to *finite fields* (but it was shown in [6] and [7] that they cannot be generalized to $\mathbb{Z}_m$ with composite m), and we will *extend them in various directions.*

Our results will be based on certain character sum estimates of independent interest which will be collected here in Part I of the series. (In Part II, to be submitted soon to this journal, we will study algebraic equations like (1.3) and (1.4) where each of the variables is restricted to a large subset of $\mathbb{F}_q$ in the above sense, while in Part III we will study hybrid problems where some variables are taken from certain special fixed sets.) Some of these character sum estimates will have the same flavor as the problems described above in the sense that these sums will involve at least one summation of form $\sum_{a\in\mathcal{A}}$ where $\mathcal{A}$ is a "large" but otherwise unspecified subset of $\mathbb{F}_q$. Our character sum estimates and also other results in Parts II and III will generalize several earlier (sometimes classical) results. We will also use some of these estimates (mostly Theorems 4 and 5) in other papers written on 2-dimensional pseudorandom binary lattices.

Throughout this paper we will use the following notations: We consider finite fields $\mathbb{F}_q$ with order $q = p^r$. We write $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. ψ always denotes an additive, χ a multiplicative character of $\mathbb{F}_q$. We set $\chi(0) = 0$. The trivial additive character is denoted by ψ_0, the trivial (principal) multiplicative character by χ_0. The canonical additive character is denoted by ψ_1. If χ is a multiplicative and ψ an additive character of $\mathbb{F}_q$ then $G(\chi,\psi)$ denotes the Gaussian sum

$$G(\chi,\psi) = \sum_{x\in\mathbb{F}_q^*} \chi(x)\psi(x).$$

We write $e^{2\pi i\alpha} = e(\alpha)$ and $e\left(\frac{n}{p}\right) = e_p(n)$. $\mathbb{N}$ denotes the set of the positive integers and $\mathbb{Z}$ is the set of the integers.

2 Vinogradov's lemma in finite fields

If $m \in \mathbb{N}$, $a \in \mathbb{Z}$ and $\alpha(x), \beta(x)$ are complex valued functions on $\{0, 1, \ldots, m-1\}$, then by Vinogradov's lemma we have

$$\left| \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} \alpha(x)\beta(y) e_m(axy) \right| \leq (XYm)^{1/2}$$

with

$$X = \sum_{x=0}^{m-1} |\alpha(x)|^2, \qquad Y = \sum_{y=0}^{m-1} |\beta(y)|^2.$$

Indeed, this is Lemma 10a in [9], and it plays a crucial role in Vinogradov's exponential sum estimates. This lemma can be generalized easily to finite fields:

Theorem 1 *If $\alpha(x)$, $\beta(x)$ are complex valued functions on $\mathbb{F}_q$ and $\psi(x)$ is a nontrivial additive character of $\mathbb{F}_q$, then writing*

$$S = \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \alpha(x)\beta(y)\psi(xy),$$

$$X = \sum_{x \in \mathbb{F}_q} |\alpha(x)|^2 \quad \textit{and} \quad Y = \sum_{y \in \mathbb{F}_q} |\beta(y)|^2,$$

we have

$$|S| \leq (XYq)^{1/2}.$$

We remark that the $q = p$, $\alpha(x) = \beta(x) = \left(\frac{x}{p}\right)$ special case (when this upper bound is achieved) shows that in general this upper bound cannot be improved.

If $\alpha(x)$, $\beta(x)$ are the characteristic functions of the subsets $\mathcal{A}$, $\mathcal{B}$ of $\mathbb{F}_q$, then it follows that

Corollary 1 *If $\mathcal{A}$, $\mathcal{B} \subseteq \mathbb{F}_q$ and ψ is a nontrivial additive character of $\mathbb{F}_q$, then we have*

$$\left| \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \psi(ab) \right| \leq (|\mathcal{A}|\,|\mathcal{B}|\,q)^{1/2}.$$

Proof of Theorem 1. By Cauchy's inequality we have

$$\begin{aligned}|S|^2 &= \left|\sum_{x\in\mathbb{F}_q}\alpha(x)\sum_{y\in\mathbb{F}_q}\beta(y)\psi(xy)\right|^2\\ &\le \left(\sum_{x\in\mathbb{F}_q}|\alpha(x)|^2\right)\left(\sum_{x\in\mathbb{F}_q}\left|\sum_{y\in\mathbb{F}_q}\beta(y)\psi(xy)\right|^2\right)\\ &= X\left(\sum_{y_1\in\mathbb{F}_q}\sum_{y_2\in\mathbb{F}_q}\beta(y_1)\overline{\beta(y_2)}\sum_{x\in\mathbb{F}_q}\psi(x(y_1-y_2))\right).\end{aligned}$$

The last sum is q if $y_1 = y_2$ and 0 otherwise, thus it follows that

$$|S|^2 \le X\sum_{y\in\mathbb{F}_q}|\beta(y)|^2 q = XYq$$

which completes the proof of Theorem 1.

3 The dual of Vinogradov's lemma

We will prove:

Theorem 2 *If $\alpha(x)$, $\beta(x)$ are complex valued functions on $\mathbb{F}_q$ and χ is a nontrivial multiplicative character of $\mathbb{F}_q$, then writing*

$$S = \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\alpha(x)\beta(y)\chi(x+y),$$

$$X = \sum_{x\in\mathbb{F}_q}|\alpha(x)|^2 \quad \textit{and} \quad Y = \sum_{y\in\mathbb{F}_q}|\beta(y)|^2,$$

we have

$$|S| \le (XYq)^{1/2}.$$

The $q = p$, $\alpha(x) = \beta(x) = e\left(\frac{x}{p}\right)$ special case shows that in general this upper bound cannot be improved.

If $\alpha(x)$, $\beta(x)$ are the characteristic functions of the subsets $\mathcal{A}$, $\mathcal{B}$ of $\mathbb{F}_q$, then it follows that

Corollary 2 *If $\mathcal{A},\ \mathcal{B} \subseteq \mathbb{F}_q$ and χ is a nontrivial multiplicative character of $\mathbb{F}_q$, then we have*

$$\left| \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(a+b) \right| \leq \left(|\mathcal{A}|\, |\mathcal{B}|\, q \right)^{1/2}.$$

In the $q = p$ special case this is a result of Erdős and Shapiro [2]. Similar estimates also occur in [1] and [3].

Another consequence of Theorem 2 is:

Corollary 3 *If $\mathcal{A},\ \mathcal{B} \subseteq \mathbb{F}_q$, χ is a nontrivial multiplicative character of $\mathbb{F}_q$, $f(x) \in \mathbb{F}_q[x]$ and $g(x) \in \mathbb{F}_q[x]$ are not identically constant polynomials of degree F, resp. G, then we have*

$$\left| \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(f(a) + g(b)) \right| \leq \left(FG\, |\mathcal{A}|\, |\mathcal{B}|\, q \right)^{1/2}.$$

Proof of Corollary 3. Now we use Theorem 2 with $\alpha(x)$, $\beta(x)$ defined as

$$\alpha(x) = |\{a : a \in \mathcal{A},\ f(a) = x\}|$$

and

$$\beta(x) = |\{b : b \in \mathcal{B},\ g(b) = x\}|.$$

Then we have

$$X = \sum_{x \in \mathbb{F}_q} |\alpha(x)|^2 \leq \max_{x \in \mathbb{F}_q}\ \alpha(x) \sum_{x \in \mathbb{F}_q} \alpha(x) \leq F\, |\mathcal{A}|$$

and similarly,

$$Y \leq G\, |\mathcal{B}|,$$

whence the result follows.

Proof of Theorem 2. Since we defined $\chi(0)$ by 0 and $\chi \neq \chi_0$ is assumed, thus we have

$$\chi(x+y) = \frac{1}{q} \sum_{\psi} G(\chi, \overline{\psi}) \psi(x+y).$$

It follows that

$$\begin{aligned} S &= \frac{1}{q}\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\alpha(x)\beta(y)\sum_{\psi}G(\chi,\overline{\psi})\psi(x+y) \\ &= \frac{1}{q}\sum_{\psi}G(\chi,\overline{\psi})\left(\sum_{x\in\mathbb{F}_q}\alpha(x)\psi(x)\right)\left(\sum_{y\in\mathbb{F}_q}\beta(y)\psi(y)\right) \\ &= \frac{1}{q}\left(G(\chi,\psi_0)+\sum_{\psi\neq\psi_0}G(\chi,\overline{\psi})\right)\left(\sum_{x\in\mathbb{F}_q}\alpha(x)\psi(x)\right)\left(\sum_{y\in\mathbb{F}_q}\beta(y)\psi(y)\right). \end{aligned}$$

By $\chi \neq \chi_0$ we have

$$G(\chi,\psi_0) = 0$$

and

$$\left|G(\chi,\overline{\psi})\right| = q^{1/2} \qquad \text{if } \psi \neq \psi_0.$$

Thus by Cauchy's inequality

$$\begin{aligned} |S| &\le \frac{1}{q}\sum_{\psi\neq\psi_0}\left|G(\chi,\overline{\psi})\right|\left|\sum_{x\in\mathbb{F}_q}\alpha(x)\psi(x)\right|\left|\sum_{y\in\mathbb{F}_q}\beta(y)\psi(y)\right| \\ &= \frac{1}{q^{1/2}}\sum_{\psi\neq\psi_0}\left|\sum_{x\in\mathbb{F}_q}\alpha(x)\psi(x)\right|\left|\sum_{y\in\mathbb{F}_q}\beta(y)\psi(y)\right| \\ &\le \frac{1}{q^{1/2}}\left(\sum_{\psi\neq\psi_0}\left|\sum_{x\in\mathbb{F}_q}\alpha(x)\psi(x)\right|^2\right)^{1/2}\left(\sum_{\psi\neq\psi_0}\left|\sum_{y\in\mathbb{F}_q}\beta(y)\psi(y)\right|^2\right)^{1/2}. \end{aligned} \tag{3.1}$$

Here we have

$$\begin{aligned} &\sum_{\psi\neq\psi_0}\left|\sum_{x\in\mathbb{F}_q}\alpha(x)\psi(x)\right|^2 \le \sum_{\psi}\left|\sum_{x\in\mathbb{F}_q}\alpha(x)\psi(x)\right|^2 \\ &= \sum_{\psi}\sum_{x_1\in\mathbb{F}_q}\sum_{x_2\in\mathbb{F}_q}\alpha(x_1)\overline{\alpha(x_2)}\psi(x_1-x_2) = q\sum_{x\in\mathbb{F}_q}|\alpha(x)|^2 = qX. \end{aligned} \tag{3.2}$$

Similarly

$$\sum_{\psi\neq\psi_0}\left|\sum_{y\in\mathbb{F}_q}\beta(y)\psi(y)\right|^2 \le qY. \tag{3.3}$$

It follows from (3.1), (3.2) and (3.3) that

$$|S| \le (qXY)^{1/2}.$$

4 The multiplicative analog of Theorem 2

We will also need the analog of Theorem 2 with $xy+1$ in place of $x+y$:

Theorem 3 *If $\alpha(x)$, $\beta(x)$ are complex valued functions on $\mathbb{F}_q$ and χ is a nontrivial multiplicative character of $\mathbb{F}_q$, then writing*

$$S = \sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q} \alpha(x)\beta(y)\chi(xy+1),$$

$$X = \sum_{x\in\mathbb{F}_q^*} |\alpha(x)|^2 \quad \textit{and} \quad Y = \sum_{y\in\mathbb{F}_q} |\beta(y)|^2,$$

we have

$$|S| \le (XYq)^{1/2}. \tag{4.1}$$

The $q=p$, $\alpha(x) = \chi(x^{-1})e\left(\frac{x^{-1}}{p}\right)$, $\beta(y) = \left(\frac{y}{p}\right)$ special case shows that the upper bound cannot be improved by more than a secondary term $(XY)^{1/2}q^{-1/2}$.

If $\alpha(x), \beta(x)$ are the characteristic functions of the subsets $\mathcal{A} \subseteq \mathbb{F}_q^*$, $\mathcal{B} \subseteq \mathbb{F}_q$, then it follows that

Corollary 4 *If $\mathcal{A} \subseteq \mathbb{F}_q^*$, , $\mathcal{B} \subseteq \mathbb{F}_q$ and χ is a nontrivial multiplicative character of $\mathbb{F}_q$, then we have*

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}} \chi(ab+1)\right| \le \left(|\mathcal{A}|\,|\mathcal{B}|\,q\right)^{1/2}.$$

The $q=p$ special case of this is a variant of Gyarmati's Theorem 7.a) in [4], and the $q=p$, $\chi(n) = \left(\frac{n}{p}\right)$ (=Legendre symbol) special case occurs in Vinogradov's book [10].

We remark that the summation over $x \in \mathbb{F}_q^*$ in Theorem 3 can be changed easily at the expense of adding a further term for summation over $x \in \mathbb{F}_q$. Indeed, by Theorem 3 we have

$$\begin{aligned}
&\left|\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\alpha(x)\beta(y)\chi(xy+1)\right| \\
\leq &\left|\sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q}\alpha(x)\beta(y)\chi(xy+1)\right| + |\alpha(0)|\sum_{y\in\mathbb{F}_q}|\beta(y)| \\
\leq &(XYq)^{1/2} + |\alpha(0)|\left(\sum_{y\in\mathbb{F}_q}|\beta(y)|^2\right)^{1/2} q^{1/2} = \left(X^{1/2}+|\alpha(0)|\right)(Yq)^{1/2}
\end{aligned}$$

so that it follows from Theorem 3:

Theorem 3' *Defining $\alpha(x)$, $\beta(x)$, χ, X and Y as in Theorem 3, we have*

$$\left|\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\alpha(x)\beta(y)\chi(xy+1)\right| \leq \left(X^{1/2}+|\alpha(0)|\right)(Yq)^{1/2}.$$

In the same way as Corollary 3 follows from Theorem 2, it follows from Theorem 3':

Corollary 5 *If $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$, χ is a nontrivial multiplicative character of $\mathbb{F}_q$, $f(x) \in \mathbb{F}_q[x]$ and $g(x) \in \mathbb{F}_q[x]$ are not identically constant polynomials of degree F, resp. G, then we have*

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\chi(f(a)g(b)+1)\right| \leq \left((F|\mathcal{A}|)^{1/2}+F\right)(G|\mathcal{B}|q)^{1/2}.$$

Proof of Theorem 3. The theorem is nearly equivalent with Theorem 2. Indeed, in Theorem 2 taking $\alpha(0) = 0$ and for $x \neq 0$ replacing $\alpha(x)$ by $\alpha(x^{-1})\chi(x^{-1})$, then substituting $x^{-1} = z$ we get

$$\sum_{z\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q}\alpha(z)\beta(y)\chi(zy+1)$$

which proves the result (with z in place of x).

5 A generalization of Vinogradov's lemma

One might like to generalize Theorems 1, 2 and 3 by estimating double sums with general term $\alpha(x)\beta(y)\psi(f(x,y))$ resp. $\alpha(x)\beta(y)\chi(f(x,y))$ with $f(x,y) \in \mathbb{F}_q[x,y]$. First we will prove such a theorem in case of additive characters ψ, i.e., we will generalize Vinogradov's lemma. However, there will be a price paid for the greater generality: we will need further assumptions, we will use Weil's theorem and the upper bound will be weaker.

Theorem 4 *Assume that $\alpha(x), \beta(x)$ are complex valued functions on $\mathbb{F}_q$, ψ is a nontrivial additive character of $\mathbb{F}_q$, $f(x,y) \in \mathbb{F}_q[x,y]$, and $f(x,y)$ is not of the form $g(x)+h(y)$:*

$$f(x,y) \neq g(x)+h(y) \quad \textit{(with } g(x), h(x) \in \mathbb{F}_q[x]\textit{)}. \tag{5.1}$$

Write $f(x,y)$ in the form

$$f(x,y) = \sum_{k=0}^{n} g_k(y)x^k \tag{5.2}$$

(with $g_k(y) \in \mathbb{F}_q[y]$), and let K denote the greatest value k with the property that $g_k(y)$ is not identically constant: $g_k(y) \not\equiv c$ and either $K = n$ or $g_{K+1}(y), g_{K+2}(y), \ldots, g_n(y)$ are identically constant so that, by (5.1),

$$K > 0. \tag{5.3}$$

Denote the degree of the polynomial $g_K(y)$ by D so that

$$D > 0, \tag{5.4}$$

and assume that

$$(K,q) = 1. \tag{5.5}$$

Write

$$S = \sum_{x\in\mathbb{F}_q} \sum_{y\in\mathbb{F}_q} \alpha(x)\beta(y)\psi(f(x,y)), \tag{5.6}$$

$$X = \sum_{x \in \mathbb{F}_q} |\alpha(x)|^2 \quad \textit{and} \quad Y = \sum_{y \in \mathbb{F}_q} |\beta(y)|^2 .$$

Then we have

$$|S| \le \left(XYq \left(D + (K-1)q^{1/2} \right) \right)^{1/2} . \tag{5.7}$$

Remarks. Condition (5.1) is necessary: if $f(x,y) = g(x) + h(y)$, then taking $\alpha(x) = \psi(-g(x))$, $\beta(y) = \psi(-h(y))$, every term of the sum (5.6) is 1, so that in general there is no nontrivial upper bound for the sum (5.6).

Condition (5.5) is an inconvenient one but a condition of this type is also necessary; we will return to this question after Lemma 1. However, in the most important special case $r = 1$, i.e., $q = p^r = p$ =prime this condition can be dropped. Namely, then using $x^p = x$ we may reduce the exponents of x in (5.2) to exponents less than p, which implies that $K < p$ whence

$$(K, q) = (K, p) = 1$$

follows so that (5.5) automatically holds. Thus in the $q = p$ special case (5.1) is the only condition that we need.

Again Theorem 4 could be specified to the case when $\alpha(x)$, $\beta(x)$ are the characteristic functions of subsets $\mathcal{A}$, $\mathcal{B}$ of $\mathbb{F}_q$, we leave the details to the reader.

Proof of Theorem 4. By Cauchy's inequality we have

$$\begin{aligned} |S|^2 &= \left| \sum_{x \in \mathbb{F}_q} \alpha(x) \sum_{y \in \mathbb{F}_q} \beta(y) \psi(f(x,y)) \right|^2 \\ &\le \left(\sum_{x \in \mathbb{F}_q} |\alpha(x)|^2 \right) \left(\sum_{x \in \mathbb{F}_q} \left| \sum_{y \in \mathbb{F}_q} \beta(y) \psi(f(x,y)) \right|^2 \right) \\ &= X \left(\sum_{x \in \mathbb{F}_q} \sum_{y_1 \in \mathbb{F}_q} \sum_{y_2 \in \mathbb{F}_q} \beta(y_1) \overline{\beta(y_2)} \psi(f(x,y_1) - f(x,y_2)) \right) \\ &= XS' \end{aligned} \tag{5.8}$$

where

$$S' = \sum_{y_1 \in \mathbb{F}_q} \sum_{y_2 \in \mathbb{F}_q} \beta(y_1)\overline{\beta(y_2)} \sum_{x \in \mathbb{F}_q} \psi\left(\sum_{k=0}^{K} (g_k(y_1) - g_k(y_2))x^k\right).$$

Now we introduce an equivalence relation in $\mathbb{F}_q$: we say that $y_1 \sim y_2$ if $g_K(y_1) = g_K(y_2)$. Then we may write $\mathbb{F}_q$ as the disjoint union of equivalence classes: $\mathbb{F}_q = \cup_{t=1}^{T} E_t$. The polynomial $g_K(y)$ may assume any fixed value at most D times so that

$$|E_t| \le D \text{ for } 1 \le t \le T. \tag{5.9}$$

We split the sum S' into two parts:

$$S' = S_1 + S_2 \tag{5.10}$$

where in S_1 we sum over the pairs (y_1, y_2) with $y_1 \sim y_2$ and S_2 denotes the sum with $y_1 \not\sim y_2$. In S_1 we estimate in the trivial way by using $|\psi(\dots)| = 1$ and (5.9):

$$\begin{aligned} |S_1| &\le \sum_{\substack{y_1, y_2 \in \mathbb{F}_q \\ y_1 \sim y_2}} |\beta(y_1)\beta(y_2)| \sum_{x \in \mathbb{F}_q} 1 = q \sum_{t=1}^{T} \sum_{y_1 \in E_t} \sum_{y_2 \in E_t} |\beta(y_1)\beta(y_2)| \\ &\le q \sum_{t=1}^{T} \sum_{y_1 \in E_t} \sum_{y_2 \in E_t} \frac{1}{2}\left(|\beta(y_1)|^2 + |\beta(y_2)|^2\right) = q \sum_{t=1}^{T} |E_t| \sum_{y \in E_t} |\beta(y)|^2 \\ &\le qD \sum_{y \in \mathbb{F}_q} |\beta(y)|^2 = qDY. \end{aligned} \tag{5.11}$$

To estimate S_2 we need the following form of the Weil's theorem ([11], see also [5], p. 223):

Lemma 1 *Let $h(x) \in \mathbb{F}_q[x]$ be of degree $d \ge 1$ with*

$$(d, q) = 1 \tag{5.12}$$

and let ψ be a nontrivial additive character of $\mathbb{F}_q$. Then

$$\left|\sum_{x \in \mathbb{F}_q} \psi(h(x))\right| \le (d-1)q^{1/2}.$$

We remark that the necessity of condition (5.12) is discussed in [5], p. 223, and this discussion also shows that condition (5.5) is needed in Theorem 4.

By using Lemma 1 we obtain

$$\begin{aligned}|S_2| &\le \sum_{\substack{y_1,y_2\in\mathbb{F}_q\\ y_1\not\sim y_2}} |\beta(y_1)\beta(y_2)| \left|\sum_{x\in\mathbb{F}_q} \psi\left(\sum_{n=0}^{K}(g_n(y_1)-g_n(y_2))x^n\right)\right| \\ &\le (K-1)q^{1/2}\sum_{y_1\in\mathbb{F}_q}\sum_{y_2\in\mathbb{F}_q}\frac{1}{2}\left(|\beta(y_1)|^2+|\beta(y_2)|^2\right) \\ &= Y(K-1)q^{3/2}. \end{aligned} \tag{5.13}$$

It follows from (5.8), (5.10), (5.11) and (5.13) that

$$|S|^2 \le XYq(D+(K-1)q^{1/2})$$

which completes the proof of Theorem 4.

6 A general theorem in case of multiplicative characters

In this section we will prove the analog of Theorem 4 for multiplicative characters, i.e., we will estimate double sums of form (5.6) with a multiplicative character χ in place of ψ. Before formulating our result, we need a little preparation. First we will present an analog of the notion of primitive polynomial used in the study of irreducibility in $\mathbb{Z}[x]$:

Definition 1 *A polynomial*

$$F(x,y)=\sum_{i=0}^{n}G_i(y)x^i=\sum_{j=0}^{m}H_j(x)y^j\in\mathbb{F}_q[x,y]$$

is said to be <u>*primitive in x*</u> *if* $(G_0(y),\dots,G_n(y))=1$, *and it is said to be* <u>*primitive in y*</u> *if* $(H_0(x),\dots,H_m(x))=1$.

Then the analog of Gauss's lemma (the product of primitive polynomials is also primitive in $\mathbb{Z}[x]$) holds.

Lemma 2 *If the polynomials*

$$F(x,y) = a_r(y)x^r + \cdots + a_0(y)$$
$$G(x,y) = b_s(y)x^s + \cdots + b_0(y)$$

are primitive in x, then the polynomial

$$H(x,y) = F(x,y)G(x,y) = c_{r+s}(y)x^{r+s} + \cdots + c_0(y)$$

is also primitive in x.

Proof of Lemma 2. The proof is similar to the proof of Gauss's lemma, i.e., we prove by contradiction: Assume that $H(x,y)$ is not primitive in x: $(c_{r+s}(y), \ldots, c_0(y)) \neq 1$. Then $c_{r+s}(y), \ldots, c_0(y)$ have a common zero $y_0 \in \overline{\mathbb{F}_q}$. Since $F(x,y)$ and $G(x,y)$ are primitive in x, thus there are n and m with $0 \leq n \leq r$ and $0 \leq m \leq s$ such that $a_i(y_0) = 0$ for $0 \leq i < n$, $a_n(y_0) \neq 0$, $b_j(y_0) = 0$ for $0 \leq j < m$, and $b_m(y_0) \neq 0$. Then we have

$$c_{n+m}(y_0) = \sum_{i=0}^{n+m} a_i(y_0)b_{n+m-i}(y_0).$$

On the right hand side every term is zero except for the term $a_n(y_0)b_m(y_0)$ which is nonzero, thus the left hand side is also nonzero: $c_{n+m}(y_0) \neq 0$. This contradicts the definition of y_0, and the proof of Lemma 2 is completed.

Now consider a polynomial

$$f(x,y) = a_r(x)y^r + \cdots + a_0(x) \in \mathbb{F}_q[x,y].$$

Then factoring out the greatest common divisor $F(x) = (a_r(x), \ldots, a_0(x))$, reordering the terms according to the powers of x, and then factoring out the greatest common divisor $G(y)$ of the coefficients (which are polynomials in y), we obtain the representation of $f(x,y)$ in the form

$$f(x,y) = F(x)G(y)H(x,y) \tag{6.1}$$

where $H(x,y) \in \mathbb{F}_q[x,y]$ is primitive in both x and y, (the primitivity in y holds trivially since $G(y)$ has been factored out, while the primitivity in x needs a little consideration: a polynomial $F(x,y) \in \mathbb{F}_q[x,y]$ is primitive in x if and only if there is no $y_0 \in \overline{\mathbb{F}}_q$ such that $F(x,y_0) \in \mathbb{F}_q[x]$ is the identically zero polynomial. Thus by (6.1) there is no $y_0 \in \overline{\mathbb{F}}_q$ such that for $y = y_0$ the polynomial $G(y)H(x,y)$ is the identically zero polynomial. Then the same holds for the polynomial $H(x,y)$, and thus it is primitive in x.) It is easy to see that apart from constant factors, this representation is unique.

Proposition 1 *Every polynomial $f(x,y) \in \mathbb{F}_q[x,y]$ can be written in form* (6.1) *where $H(x,y)$ is primitive in both x and y and apart from constant factors, this representation is unique.*

Definition 2 *The polynomial $H(x,y)$ in* (6.1) *(which is determined uniquely apart from a constant factor) will be called the primitive kernel of $f(x,y)$.*

Theorem 5 *Assume that $\alpha(x), \beta(x)$ are complex valued functions on $\mathbb{F}_q$, χ is a nontrivial multiplicative character of $\mathbb{F}_q$ of order d, $f(x,y) \in \mathbb{F}_q[x,y]$, the primitive kernel $H(x,y)$ of $f(x,y)$ is not of the form $cK(x,y)^d$:*

$$H(x,y) \neq cK(x,y)^d \text{ for } c \in \mathbb{F}_q,\ K(x,y) \in \mathbb{F}_q[x,y], \tag{6.2}$$

and $f(x,y)$ is of degree n and m in x, resp. y. Then, writing

$$S = \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \alpha(x)\beta(y)\chi(f(x,y)),$$

$$X = \sum_{x \in \mathbb{F}_q} |\alpha(x)|^2,\ Y = \sum_{y \in \mathbb{F}_q} |\beta(y)|^2$$

and

$$B = \max_{y \in \mathbb{F}_q} |\beta(y)|,$$

we have

$$|S| < (X(2nYq^{3/2} + 5B^2nmq^2))^{1/2}. \tag{6.3}$$

We remark that it is easy to see that the condition (6.2) is also necessary. Indeed, if this condition does not hold then there exist functions $\alpha(x)$, $\beta(x)$ so that S is large.

Proof of Theorem 5. By Cauchy's inequality we have

$$\begin{aligned}
\left|S^2\right| &= \left|\sum_{x\in\mathbb{F}_q}\alpha(x)\sum_{y\in\mathbb{F}_q}\beta(y)\chi(f(x,y))\right|^2 \\
&\le \left(\sum_{x\in\mathbb{F}_q}|\alpha(x)|^2\right)\left(\sum_{x\in\mathbb{F}_q}\left|\sum_{y\in\mathbb{F}_q}\beta(y)\chi(f(x,y))\right|^2\right) \\
&= X\left(\sum_{x\in\mathbb{F}_q}\sum_{y_1\in\mathbb{F}_q}\sum_{y_2\in\mathbb{F}_q}\beta(y_1)\overline{\beta(y_2)}\chi(f(x,y_1))\overline{\chi}(f(x,y_2))\right) \\
&= XS' \qquad (6.4)
\end{aligned}$$

where using representation (6.1) of $f(x,y)$

$$\begin{aligned}
S' &= \sum_{y_1\in\mathbb{F}_q}\sum_{y_2\in\mathbb{F}_q}\beta(y_1)\overline{\beta(y_2)}\sum_{x\in\mathbb{F}_q}\chi(f(x,y_1)f^{d-1}(x,y_2)) \\
&= \sum_{y_1\in\mathbb{F}_q}\sum_{y_2\in\mathbb{F}_q}\beta(y_1)\overline{\beta(y_2)}\sum_{x\in\mathbb{F}_q}\chi\left(F^d(x)G(y_1)G^{d-1}(y_2)H(x,y_1)H^{d-1}(x,y_2)\right) \\
&= \sum_{y_1\in\mathbb{F}_q}\sum_{y_2\in\mathbb{F}_q}\beta(y_1)\overline{\beta(y_2)}\chi\left(G(y_1)G^{d-1}(y_2)\right)\sum_{\substack{x\in\mathbb{F}_q\\F(x)\neq 0}}\chi\left(H(x,y_1)H^{d-1}(x,y_2)\right)
\end{aligned} \qquad (6.5)$$

whence

$$|S'| \le \sum_{y_1\in\mathbb{F}_q}\sum_{y_2\in\mathbb{F}_q}|\beta(y_1)\beta(y_2)|\left|\sum_{\substack{x\in\mathbb{F}_q\\F(x)\neq 0}}\chi(H(x,y_1)H^{d-1}(x,y_2))\right|. \qquad (6.6)$$

Now we introduce the following notations: write

$$\mathcal{Y} = \{(y_1,y_2) : y_1\in\mathbb{F}_q,\ y_2\in\mathbb{F}_q\},$$

let $\mathcal{Y}_1$ denote the set of the elements $y_0 \in \mathbb{F}_q$ such that $H(x, y_0)$ is of form $H(x, y_0) = ch^d(x)$ with $c \in \mathbb{F}_q$, $h(x) \in \mathbb{F}_q[x]$:

$$\mathcal{Y}_1 = \{y_0 \in \mathbb{F}_q : \exists\, c \in \mathbb{F}_q,\ h(x) \in \mathbb{F}_q[x] \text{ such that } H(x, y_0) = ch^d(x)\},$$

and let $\mathcal{Y}_2$ denote the set of the pairs $(y_1, y_2) \in \mathcal{Y}$ such that $y_1 \notin \mathcal{Y}_1$, $y_2 \notin \mathcal{Y}_1$, and $H(x, y_1)$ and $H(x, y_2)$ have a common zero or, equivalently,

$$\deg(H(x, y_1), H(x, y_2)) > 0 \tag{6.7}$$

(note that it follows from $y_1 \notin \mathcal{Y}_1$, $y_2 \notin \mathcal{Y}_1$) that $H(x, y_1)$ and $H(x, y_2)$ are not identically constant). If

$$(y_1, y_2) \in \mathcal{Y},\ y_1 \notin \mathcal{Y}_1,\ y_2 \notin \mathcal{Y}_1,\ (y_1, y_2) \notin \mathcal{Y}_2, \tag{6.8}$$

then clearly $H(x, y_1)H^{d-1}(x, y_2)$ is not of the form $ch^d(x)$ with $c \in \mathbb{F}_q$, $h(x) \in \mathbb{F}_q[x]$. Thus we may use Weil's theorem to estimate the innermost sum in (6.6):

Lemma 3 *Suppose χ is a multiplicative character of order $d > 1$ over $\mathbb{F}_q$. Suppose $f(x) \in \mathbb{F}_q[x]$ has s distinct zeros over the algebraic closure of $\mathbb{F}_q$, and it is not the constant multiple of the d-th power of a polynomial over $\mathbb{F}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq (s-1)q^{1/2}.$$

Proof of Lemma 3. This is Weil's theorem [11] (see also [8, p. 43]).

We will prove that

$$\left| \sum_{\substack{x \in \mathbb{F}_q \\ F(x) \neq 0}} \chi(H(x, y_1)H^{d-1}(x, y_2)) \right| < 2nq^{1/2} \tag{6.9}$$

for every pair (y_1, y_2) satisfying (6.8). Indeed, if $n > q^{1/2}/2$, then (6.9) trivially holds. For $n \leq q^{1/2}/2$ we will use the triangle-inequality and Lemma

3. Since now both $H(x, y_1)$ and $H(x, y_2)$ have at most n distinct zeros, thus we have

$$\left| \sum_{\substack{x \in \mathbb{F}_q \\ F(x) \neq 0}} \chi(H(x, y_1) H^{d-1}(x, y_2)) \right| \leq \left| \sum_{x \in \mathbb{F}_q} \chi(H(x, y_1) H^{d-1}(x, y_2)) \right| + \sum_{F(x)=0} 1$$
$$\leq (2n-1) q^{1/2} + n < 2nq^{1/2}.$$

Thus the contribution of the pairs (y_1, y_2) satisfying (6.8) to the sum (6.6) is

$$\begin{aligned} S_1 &= \sum_{\substack{(y_1, y_2) \in \mathcal{Y} \setminus \mathcal{Y}_2 \\ y_1, y_2 \notin \mathcal{Y}_1}} |\beta(y_1)\beta(y_2)| \left| \sum_{\substack{x \in \mathbb{F}_q \\ F(x) \neq 0}} \chi(H(x, y_1) H^{d-1}(x, y_2)) \right| \\ &< \sum_{(y_1, y_2) \in \mathcal{Y}} |\beta(y_1)\beta(y_2)| \, 2nq^{1/2} \\ &\leq 2nq^{1/2} \sum_{y_1 \in \mathbb{F}_q} \sum_{y_2 \in \mathbb{F}_q} \frac{1}{2} \left(|\beta(y_1)|^2 + |\beta(y_2)|^2 \right) \\ &= 2nYq^{3/2}. \end{aligned} \tag{6.10}$$

If a pair $(y_1, y_2) \in \mathcal{Y}$ does not satisfy (6.8) then we use the trivial estimate

$$|\beta(y_1)\beta(y_2)| \left| \sum_{\substack{x \in \mathbb{F}_q \\ F(x) \neq 0}} \chi(H(x, y_1) H^{d-1}(x, y_2)) \right| \leq B^2 q$$

and the number of these pairs is

$$\begin{aligned} &\leq |\{(y_1, y_2) \in \mathcal{Y} : \ y_1 \in \mathcal{Y}_1\}| + |\{(y_1, y_2) \in \mathcal{Y} : \ y_2 \in \mathcal{Y}_1\}| + |(y_1, y_2) \in \mathcal{Y}_2| \\ &= 2q \, |\mathcal{Y}_1| + |\mathcal{Y}_2| \end{aligned}$$

so that the total contribution of these pairs to the sum (6.6) is

$$S_2 \leq (2q \, |\mathcal{Y}_1| + |\mathcal{Y}_2|) \, B^2 q. \tag{6.11}$$

It remains to estimate $|\mathcal{Y}_1|$ and $|\mathcal{Y}_2|$.

Lemma 4 *Using the notations above, we have*

$$|\mathcal{Y}_1| \leq nm + m. \tag{6.12}$$

Proof of Lemma 4. Write $H(x, y)$ in form

$$H(x, y) = p_n(y)x^n + \cdots + p_1(y)x + p_0(y) \tag{6.13}$$

(with $p_i(y) \in \mathbb{F}_q[y]$ for $i = 0, 1, \ldots, n$), and define $\mathcal{Y}_3,\ \mathcal{Y}_4$ by

$$\mathcal{Y}_3 = \{y :\ y \in \mathcal{Y}_1,\ p_n(y) = 0\}$$

and

$$\mathcal{Y}_4 = \{y :\ y \in \mathcal{Y}_1,\ p_n(y) \neq 0\}$$

so that

$$|\mathcal{Y}_1| = |\mathcal{Y}_3| + |\mathcal{Y}_4|\,. \tag{6.14}$$

The degree of $p_n(y)$ is at most m thus clearly we have

$$|\mathcal{Y}_3| \leq m. \tag{6.15}$$

If

$$y_0 \in \mathcal{Y}_4 \tag{6.16}$$

then $H(x, y_0)$ is of the form

$$H(x, y_0) = ch^d(x). \tag{6.17}$$

If the coefficient of the highest degree term of $h(x)$ is C, then (6.17) can be rewritten as

$$H(x, y_0) = c_0 C^d h_0^d(x)$$

where $c_0 C^d \in \mathbb{F}_q$, $h_0(x) \in \mathbb{F}_q[x]$, and the coefficient of the highest degree term of $h_0(x)$ is 1. Thus if $y_1, y_2, \ldots, y_T$ denote the distinct elements of $\mathcal{Y}_4$, then for $i = 1, 2, \ldots, T$ the polynomial $H(x, y_i)$ can be written in form

$$H(x, y_i) = c_i h_i^d(x) \text{ with } c_i \in \mathbb{F}_q,\ h_i(x) \in \mathbb{F}_q[x], \tag{6.18}$$

where the coefficient of the highest degree term of $h_i(x)$ is 1. Then substituting $y = y_i$ in (6.13) and comparing the equation obtained with (6.18), we get that

$$c_i = p_n(y_i),$$

so that (6.18) can be rewritten as

$$H(x, y_i) = p_n(y_i)h_i^d(x),\ p_n(y_i) \in \mathbb{F}_q,\ h_i(x) \in \mathbb{F}_q[x]. \tag{6.19}$$

Denote the coefficients of the polynomial $h_i(x)$ by $a_r(i), \ldots, a_1(i), a_0(i)$:

$$h_i(x) = a_r(i)x^r + a_{r-1}(i)x^{r-1} + \cdots + a_1(i)x + a_0(i) \tag{6.20}$$

so that

$$a_r(i) = 1,\ a_{r-j}(i) \in \mathbb{F}_q \text{ (for } j = 1, \ldots, r) \text{ and } r = \frac{n}{d}. \tag{6.21}$$

Now we will prove

Lemma 5 *For every $1 \le i \le T$ and for $j = 0, 1, \ldots, r$ the coefficient $a_{r-j}(i)$ is of form*

$$a_{r-j}(i) = \frac{q_{r-j}(y_i)}{(p_n(y_i))^j}$$

where $q_{r-j}(y) \in \mathbb{F}_q[y]$ and deg $q_{r-j}(y) \le jm$.

Proof of Lemma 5. We will prove the lemma by induction on j. For $j = 0$ the assertion of the lemma holds by (6.21).

Assume now that the assertion of the lemma holds for $0, 1, \ldots, j-1$ in place of $j(\ge 1)$, and we will prove that it also holds for j.

The coefficient of x^{n-j} in $p_n(y_i)h_i^d(x)$ is

$$p_n(y_i)\left(da_{r-j}(i) + \sum_{\substack{0 \le t_0, \ldots, t_{j-1} \\ t_0 + \cdots + t_{j-1} = d \\ t_1 + 2t_2 + \cdots + (j-1)t_{j-1} = j}} \frac{d!}{t_0! \ldots t_{j-1}!} a_{r-1}(i)^{t_1} \cdots a_{r-(j-1)}(i)^{t_j}\right).$$

Applying the assumption of the induction on $a_{r-1}(i), \ldots, a_{r-(j-1)}(i)$, we obtain that the coefficient of x^{n-j} is of form

$$p_n(y_i)\left(da_{r-j}(i) + \frac{s(y_i)}{(p_n(y_i))^j}\right)$$

where the degree of the polynomial $s(y) \in \mathbb{F}_q[y]$ is $\leq jm$. On the other hand, by (6.13) and (6.19) this coefficient is the same as the coefficient of x^{n-j} in $H(x, y_i)$, i.e., $p_{n-j}(y_i)$. Thus we have

$$p_{n-j}(y_i) = p_n(y_i) \left(da_{r-j}(i) + \frac{s(y_i)}{(p_n(y_i))^j} \right)$$

whence

$$a_{r-j}(i) = \frac{p_{n-j}(y_i) p_n(y_i)^{j-1} - s(y_i)}{d(p_n(y_i))^j}$$

which completes the proof of Lemma 5. (Here we have used $(d, p) = 1$ which follows from $d \mid q - 1 = p^r - 1$.)

By (6.20) and Lemma 5, for $1 \leq i \leq T$ the polynomial $h_i(x)$ is of form

$$h_i(x) = x^r + \frac{q_{r-1}(y_i)}{p_n(y_i)} x^{r-1} + \frac{q_{r-2}(y_i)}{p_n(y_i)^2} x^{r-2} + \cdots + \frac{q_0(y_i)}{(p_n(y_i))^r} \stackrel{\text{def}}{=} h(x, y_i) \tag{6.22}$$

where the degree of the polynomial $q_{r-j}(y_i) \in \mathbb{F}_q[y]$ is $\leq jm$. It follows from (6.19) and (6.22) that

$$H(x, y_i) = p_n(y_i) h^d(x, y_i). \tag{6.23}$$

By using (6.22), we may deduce that the coefficient of x^{n-k} on the right hand side of (6.23) is of form

$$\frac{r_{n-k}(y_i)}{(p_n(y_i))^{k-1}}$$

where the degree of the polynomial $r_{n-k}(y) \in \mathbb{F}_q[y]$ is $\leq mk$. This must be equal to the coefficient of x^{n-k} on the left hand side of (6.23) which is $p_{n-k}(y_i)$ by (6.13) so that for every $1 \leq k \leq n$ we have

$$p_{n-k}(y_i) = \frac{r_{n-k}(y_i)}{(p_n(y_i))^{k-1}}$$

whence

$$p_{n-k}(y_i) \left(p_n(y_i)\right)^{k-1} - r_{n-k}(y_i) = 0. \tag{6.24}$$

Now we will prove:

Lemma 6 *There is a k with $1 \leq k \leq n$ so that*

$$p_{n-k}(y)(p_n(y))^{k-1} - r_{n-k}(y) \tag{6.25}$$

is <u>not</u> the identically zero polynomial.

Proof of Lemma 6. We will prove by contradiction: assume that

$$p_{n-k}(y)(p_n(y))^{k-1} - r_{n-k}(y) = 0 \text{ for every } 1 \leq k \leq n.$$

Then it follows from the computation above that (6.23) holds with y in place of y_i:

$$H(x,y) = p_n(y)h^d(x,y) \tag{6.26}$$

where $h(x,y)$ is the rational function defined in (6.22) so that it is of form

$$h(x,y) = \frac{k(x,y)}{(p_n(y))^r}$$

with $k(x,y) \in \mathbb{F}_q[x,y]$. Ordering $k(x,y)$ according to the powers of x and factoring out the greatest common divisor $a(y)$ of the coefficients (which are polynomials in y), we obtain that $k(x,y)$ can be written in form $k(x,y) = a(y)\ell(x,y)$ where $\ell(x,y) \in \mathbb{F}_q[x,y]$ is primitive in x. Then (6.26) can be rewritten as

$$H(x,y) = p_n(y)\left(\frac{a(y)\ell(x,y)}{(p_n(y))^r}\right)^d$$

whence

$$(p_n(y))^{rd-1}H(x,y) = (a(y))^d(\ell(x,y))^d. \tag{6.27}$$

By our assumption $H(x,y)$ is primitive in x, and by the definition of $\ell(x,y)$ and Lemma 2, $(\ell(x,y))^d$ is primitive in x. It follows that ordering these polynomials according to the powers of x and considering the greatest common divisor of the coefficients which are polynomials in y, these greatest common divisors are $(p_n(y))^{rd-1}$ resp. $(a(y))^d$, and they must be equal apart from a constant factor:

$$c\,(p_n(y))^{rd-1} = (a(y))^d. \tag{6.28}$$

It follows from (6.27) and (6.28) that

$$H(x,y) = c(\ell(x,y))^d$$

which contradicts our assumption on $H(x,y)$ in the theorem, and this completes the proof of Lemma 6.

Now consider a k with $1 \le k \le n$ for which the polynomial (6.25) is not identically zero. Then clearly, the degree of this polynomial is

$$\le \max\{(\deg\, p_{n-k}(y) + (k-1)\deg\, p_n(y))\,,\ \deg\, r_{n-k}(y)\} \le \max\{km, mk\}$$
$$\le mn.$$

By (6.24), each of the distinct elements $y_1, \ldots, y_T \in \mathbb{F}_q$ is a zero of this polynomial, thus their number is at most the degree of the polynomial, :

$$|\mathcal{Y}_4| = T \le mn. \tag{6.29}$$

(6.12) follows from (6.14), (6.15) and (6.29) and this completes the proof of Lemma 4.

Lemma 7 *Using the notations above, we have*

$$|\mathcal{Y}_2| < qnm.$$

Proof. y_1 in (6.7) can be chosen in at most q ways. If y_1 is fixed and (6.7) holds for some y_2, then the polynomials $H(x,y_1)$ and $H(x,y_2)$ have a common zero $x = \alpha$. As we have seen $H(x,y_1)$ is not identically zero, and its degree is at most the degree of $H(x,y)$ in x, i.e., it is $\le n$. Thus the zero α can be chosen in at most $\deg H(x,y_1) \le n$ ways. If y_1 and α have been fixed, then y_2 must be a zero of the polynomial $H(\alpha,y)$. If $H(\alpha,y)$ is identically 0 then $x - \alpha \mid H(x,y) - H(\alpha,y) = H(x,y)$ which contradicts the primitivity of $H(x,y)$ in y. Thus $H(\alpha,y)$ is not identically 0, its degree is at most the degree of $H(x,y)$ in y, i.e., it is $\le m$, so its zero y_2 can be chosen in at most

m ways. We may conclude that (y_1, y_2) in $\mathcal{Y}_2$ can be chosen in qnm ways which completes the proof of the lemma.

Now we can complete the proof of Theorem 5. By (6.4), (6.6), (6.10), (6.11), Lemma 4 and Lemma 7 we have

$$\begin{aligned}|S|^2 \le XS' = X(S_1+S_2) &< X\left(2nYq^{3/2} + (2q\,|\mathcal{Y}_1| + |\mathcal{Y}_2|)\,B^2q\right)\\ &\le X\left(2nYq^{3/2} + (2q(nm+m) + qnm)B^2q\right)\\ &\le X\left(2nYq^{3/2} + 5B^2nmq^2\right)\end{aligned}$$

which completes the proof of Theorem 5.

References

[1] P. Erdős and A. Sárközy, *On differences and sums of integers, I*, J. Number Theory 10 (1978), 430-450.

[2] P. Erdős and N. H. Shapiro, *On the least primitive root of a prime*, Pacific J. Math. 7 (1957), 861-865.

[3] J. Friedlander and H. Iwaniec, *Estimates for character sums*, Proc. Amer. Math. Soc. 119 (1993), 365-372.

[4] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97 (2001), 53-65.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge Univ. Press, 1997.

[6] A. Sárközy, *On sums and products of residues modulo p*, Acta Arith. 118 (2005), 403-409.

[7] A. Sárközy, *On products and shifted products of residues modulo p*, volume dedicated to the sixtieth birthday of M. B. Nathanson, Springer, to appear.

[8] W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Lecture Notes in Math. 536, Springer, New York, 1976.

[9] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, Interscience, London, 1954 (translated from Russian, the Russian original appeared in 1947).

[10] I. M. Vinogradov, *Elements of Number Theory*, Dover 1954.

[11] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publ. Inst. Math. Univ. Strasbourg 7 (1945), Hermann, Paris, 1948.

Department of Algebra and Number Theory
Eötvös Loránd University
H-1117 Budapest, Pázmány Péter sétány 1/c
Hungary
Email: sarkozy@cs.elte.hu

Alfréd Rényi Institute of Mathematics
H-1053 Reáltanoda utca 13-15
Hungary
Email: gykati@cs.elte.hu