SAVING THE LOGARITHMIC FACTOR IN THE ERROR TERM ESTIMATES OF SOME CONGRUENCE PROBLEMS

JAVIER CILLERUELO AND ANA ZUMALACÁRREGUI

Abstract. Combining previous ideas from Garaev and the first author, we prove a general theorem to estimate the number of elements of a subset A of an abelian group $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ lying in a k-dimensional box. In many cases, this approach allow us to improve, by a logarithm factor, the range where it is possible to obtain an asymptotic estimate for the number of solutions of a given congruence.

1. Introduction

Finding an asymptotic formula for the number of solutions of a given congruence is an important topic in additive number theory. One could find many examples of congruences whose solutions are well distributed and obtain asymptotic results employing exponential sums techniques. Consider, for example, the congruence

$$xy \equiv \lambda \pmod{p}, \quad x_0 + 1 \le x \le x_0 + M, \quad y_0 + 1 \le y \le y_0 + M. \tag{1}$$

The usual techniques on character sums (see for example [6]) show that, for $\lambda \not\equiv 0 \pmod{p}$, the number J_1 of solutions to (1) is given by

$$J_1 = \frac{M^2}{p} + O\big(p^{1/2}\log^2 p\big), \tag{2}$$

which provides the asymptotic formula $J_1 \sim M^2/p$ in the range $Mp^{-3/4}\log^{-2} p \to \infty$. This result was improved by Garaev [5], who obtained the error term $O(p^{1/2}\log^2(Mp^{-3/4}+3))$ and therefore extended the range for an asymptotic formula up to $Mp^{-3/4} \to \infty$.

Other example is the exponential congruence

$$g^x - g^y \equiv \lambda \pmod{p}, \quad 1 \le x, y \le M, \tag{3}$$

where g is a primitive root of $\mathbb{F}_p^*$, the multiplicative group of the finite field of p elements. As in the previous example, it is well known that, for $\lambda \not\equiv 0 \pmod{p}$, the number J_2 of solutions to (3) is given by

$$J_2 = \frac{M^2}{p} + O\big(p^{1/2}\log^2 p\big), \tag{4}$$

which also provides the asymptotic formula $J_2 \sim M^2/p$ in the range $Mp^{-3/4}\log^{-2} p \to \infty$. Garaev [5] obtained the error term $O(M^{2/3}\log^{2/3}(Mp^{-3/4}+3) + p^{1/2})$, extending the range for an asymptotic formula up to $Mp^{-3/4} \to \infty$. The same range for the asymptotic formula

is obtained by Cilleruelo [2] by showing that the error term was $O(4^r p^{1/2}((M^2p^{-3/2})^{1/r}+1))$, for any positive r. Garaev's proof exploits character sums arguments and works in $\mathbb{Z}_p$, while Cilleruelo's proof is combinatorial and works on the group $\mathbb{Z}_{p-1}\times\mathbb{Z}_{p-1}$, where the solutions to (3) live.

The combination of the ideas in [5] and [2] allow us to improve both error terms in (2) and (4), and, which is more interesting, to obtain a general result which saves the logarithmic factor in many similar situations. To motivate our result we observe that J_1 can be expressed as

$$J_1 = |A_1 \cap B_1|$$

where

$$A_1 = \{(x,y):\ xy \equiv \lambda \pmod p\} \subset G_1 = \mathbb{Z}_p \times \mathbb{Z}_p$$

and $B_1 = [x_0+1, M]\times[y_0+1, M]$, while

$$J_2 = |A_2 \cap B_2|$$

where

$$A_2 = \{(x,y) : g^x - g^y \equiv \lambda \pmod p\} \subset G_2 = \mathbb{Z}_{p-1}\times\mathbb{Z}_{p-1}$$

and $B_2 = [1,M]^2$. With this notation, Garaev's results can be expressed as

$$J_1 = |A_1\cap B_1| = \frac{|A_1||B_1|}{|G_1|} + O\left(p^{1/2}\log^2\left(|B_1|p^{-3/2}+3\right)\right) \tag{5}$$

$$J_2 = |A_2\cap B_2| = \frac{|A_2||B_2|}{|G_2|} + O\left(|B_2|^{1/3}\log^{2/3}\left(|B_2|^{1/2}p^{-3/4}+3\right)+p^{1/2}\right) \tag{6}$$

Let us now state our main theorem.

Theorem 1. *Let $G = \mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}$ be a finite abelian group, $A\subseteq G$ a subset and B a k-dimensional box in G. Then*

$$|A\cap B| = \frac{|A||B|}{|G|} + \theta|\widehat{A}|\left(1+\log_+^k\left(\tfrac{|B||A|}{|\widehat{A}||G|}\right)\right),$$

for some $|\theta|\le 100^k$, where $\log_+(x) = \max\{0,\log x\}$,

$$|\widehat{A}| = \max_{\psi\neq\psi_0}\left|\sum_{a\in A}\psi(a)\right|$$

and the sum is taken over all non principal characters in G.

In applications, A could be the set of the solutions $(x_1,\dots,x_k)$ of some equation

$$f(x_1,\dots,x_k) = 0$$

in an appropriate group G, or the points on a curve or variety defined over a finite field.

This theorem allows us to improve the error term on the asymptotic estimates obtained in many different problems. Such an improvement can be translated into the possibility of removing the logarithmic factor on the critical size of B, as in [5] was done for (5) and (6).

Observe that the error term in Theorem 1 is given in terms of $|\widehat{A}|$, therefore we must obtain good estimates for this quantity. It is easy to check that $|A|^{1/2} \leq |\widehat{A}| \leq |A|$, but in most applications A is a set with $|\widehat{A}| \ll |A|^{1/2}$.

Section 2 is dedicated to proof Theorem 1, which is stated in a very general form. Nevertheless, in Section 3 we discuss some examples of the possible applications of this result.

In some interesting situations the set A in Theorem 1 is a dense Sidon set in G: differences $a - a' : \ a \neq a', \ a, a' \in A$ are all distinct and satisfies $|A| \geq |G|^{1/2} - O(1)$. In Proposition 1 we show that $|\widehat{A}| = O(|A|^{1/2})$ for these sets. The set A_2 considered before is an example of a dense Sidon set and Theorem 1 gives an improvement on previous estimates of Garaev and Cilleruelo for the error term in this problem (see section 3.1).

In other situations the estimate of $|\widehat{A}|$ depends on deeper results. This is the case, for example, of the set A_1 considered in the congruence $xy \equiv \lambda \pmod p$, where Kloosterman sums appear. The cases where A is a plane curve or a parametrized curve will be discussed. This includes, for example, the set of points of an elliptic curve, Section 3.3, or the number of hyperelliptic curves isomorphic to a given curve with coefficients in a certain range, Section 3.2.

Finally, in Section 3.4, we illustrate how -following the same ideas- one can obtain a result analogous to Theorem 1, even if the quantity $|\widehat{A}|$ is big for a certain class of characters, and still save the logarithm factor on the range for an asymptotic result.

2. Asymptotic estimates

2.1. **Preliminaries and Notation.** For a finite abelian group $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, let us denote by ψ_α the additive character in G given by

$$\psi_\alpha(x_1, \ldots, x_k) := e\big(\tfrac{\alpha_1 x_1}{n_1} + \tfrac{\alpha_2 x_2}{n_2} + \cdots + \tfrac{\alpha_k x_k}{n_k}\big),$$

where $\alpha = (\alpha_1, \ldots, \alpha_k) \in G$ and $e(x) = e^{2\pi i x}$ for a real number x.

Observe that the notion of box will depend on how we choose to represent G as a product of cyclic groups, that choice will be connected to the specific problem we study and will not necessarily coincide with the canonical representation of G as an abelian group.

Lemma 1. *Let G be an finite abelian group. For any $A, B, C \subseteq G$ we have*

$$|\{\, (b,c) \in B \times C \, : \, b + c \in A\}| = \frac{|B||C||A|}{|G|} + \theta \, \frac{|\widehat{A}|}{|G|} \sum_{\psi \neq \psi_0} \Big| \sum_{b \in B} \psi(b) \Big| \Big| \sum_{c \in C} \psi(c) \Big|,$$

for some $|\theta| \leq 1$, where

$$|\widehat{A}| = \max_{\psi \neq \psi_0} \Big| \sum_{a \in A} \psi(a) \Big|.$$

Proof. The number of pairs $(b,c) \in B \times C$ with $b+c \in A$ is given by

$$\frac{1}{|G|}\sum_{\psi}\sum_{A,B,C}\psi(b+c-a) = \frac{|B||C||A|}{|G|} + \text{ Error},$$

where

$$\begin{aligned}|\text{Error}| &= \Big|\frac{1}{|G|}\sum_{\psi\neq\psi_0}\sum_{A,B,C}\psi(b+c-a)\Big| \\ &\leq \frac{1}{|G|}\sum_{\psi\neq\psi_0}\Big|\sum_{a\in A}\psi(-a)\Big|\Big|\sum_{b\in B}\psi(b)\Big|\Big|\sum_{c\in C}\psi(c)\Big| \\ &\leq \frac{|\widehat{A}|}{|G|}\sum_{\psi\neq\psi_0}\Big|\sum_{b\in B}\psi(b)\Big|\Big|\sum_{c\in C}\psi(c)\Big|.\end{aligned}$$

□

2.2. **Proof of Theorem 1.**

Proof. Let $B = \prod_{i=1}^{k}[H_i+1, H_i+M_i]$, $1 \leq M_i \leq n_i$, be a k-dimensional box in $G = \mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}$. Consider the following approximations of B

$$B' = \prod_{i=1}^{k}[H_i+1-m_i, H_i+M_i], \quad B'' = \prod_{i=1}^{k}[H_i+1, H_i+M_i-m_i],$$

for some suitable integers $m_i, 0 \leq m_i \leq M_i - 1$. If we denote by $C = \prod_{i=1}^{k}[0,m_i]$, then it is clear that $B \subset B'+c$ for any $c \in C$, so each element $b \in B$ has at least $|C|$ representations of the form $b = b'+c$, $b' \in B'$, $c \in C$. In particular

$$|\{(b',c) \in B'\times C,\ b'+c \in A\}| \geq |A\cap B||C|.$$

Analogously, $B''+c \subset B$ for any $c \in C$ and then

$$|\{(b'',c) \in B''\times C,\ b''+c \in A\}| \leq |A\cap B||C|.$$

Hence

$$\frac{|\{(b'',c)\in B''\times C\ : b''+c\in A\}|}{|C|} \leq |A\cap B| \leq \frac{|\{(b',c)\in B'\times C\ : b'+c\in A\}|}{|C|}.$$

In terms of Lemma 1 we have that

$$\begin{aligned}|A\cap B| &\leq \frac{1}{|C|}\Big(\frac{|A||B'||C|}{|G|} + \theta\frac{|\widehat{A}|}{|G|}\sum_{\psi\neq\psi_0}\Big|\sum_{B'}\psi(b')\Big|\Big|\sum_{C}\psi(c)\Big|\Big) \\ &\leq \frac{|A||B|}{|G|} + \frac{|A|\big(|B'|-|B|\big)}{|G|} + \frac{|\widehat{A}|}{|G||C|}\sum_{\psi}\Big|\sum_{B'}\psi(b')\Big|\Big|\sum_{C}\psi(c)\Big|, \qquad (7)\end{aligned}$$

and similarly

$$|A\cap B| \geq \frac{|A||B|}{|G|} - \frac{|A|\big(|B|-|B''|\big)}{|G|} - \frac{|\widehat{A}|}{|G||C|}\sum_{\psi}\Big|\sum_{B''}\psi(b'')\Big|\Big|\sum_{C}\psi(c)\Big|$$

$$\geq \frac{|A||B|}{|G|} - \frac{|A|\big(|B'|-|B|\big)}{|G|} - \frac{|\widehat{A}|}{|G||C|}\sum_{\psi}\Big|\sum_{B''}\psi(b'')\Big|\Big|\sum_{C}\psi(c)\Big|, \tag{8}$$

since $|B|-|B''| \leq |B'|-|B|$.

Observe that, for a fixed character $\psi_\alpha,\ \alpha=(\alpha_1,\dots,\alpha_k)$, we have

$$\sum_{b'\in B'}\psi_\alpha(b') = \prod_{i=1}^{k}\left(\sum_{b_i'=H_i+1-m_i}^{H_i+M_i} e\big(\tfrac{\alpha_i b_i'}{n_i}\big)\right),\ \sum_{b''\in B''}\psi_\alpha(b'') = \prod_{i=1}^{k}\left(\sum_{b_i''=H_i+1}^{H_i+M_i-m_i} e\big(\tfrac{\alpha_i b_i''}{n_i}\big)\right) \tag{9}$$

and

$$\sum_{c\in C}\psi_\alpha(c) = \prod_{i=1}^{k}\left(\sum_{c_i=0}^{m_i} e\big(\tfrac{\alpha_i c_i}{n_i}\big)\right).$$

For a fixed i, each sum involved is a geometric sum with ratio $e(\alpha_i/n_i)$. Whenever $\alpha_i\neq 0$, if we choose α_i to be a representative with $|\alpha_i|\leq n_i/2$, it is well known that for any a and m

$$\left|\sum_{x=a}^{a+m} e\big(\tfrac{\alpha_i x}{n_i}\big)\right| \leq \frac{2}{|1-e\big(\frac{\alpha_i}{n_i}\big)|} \leq \frac{4n_i}{|\alpha_i|},$$

and it is clear that, for any α_i including 0, this sum is bounded by $m+1$. To clear the exposition we will fix $\min\{4n_i/0, m+1\} := m+1$ and include these two facts in the following estimate

$$\left|\sum_{x=a}^{a+m} e\big(\tfrac{\alpha_i x}{n_i}\big)\right| \leq \min\left\{\tfrac{4n_i}{|\alpha_i|}, m+1\right\}, \tag{10}$$

where α_i is chosen to be the representative modulo n_i with minimum absolute value.

It follows from (9) and (10) that for every fixed $\alpha=(\alpha_1,\dots,\alpha_k)\in G,\ |\alpha_i|\leq n_i/2$, the following estimates hold

$$\Big|\sum_{B'}\psi_\alpha(b')\Big| \leq \prod_{i=1}^{k}\min\big\{\tfrac{4n_i}{|\alpha_i|}, M_i+m_i\big\} \leq \prod_{i=1}^{k}\min\big\{\tfrac{4n_i}{|\alpha_i|}, 2M_i\big\},$$

$$\Big|\sum_{B''}\psi_\alpha(b'')\Big| \leq \prod_{i=1}^{k}\min\big\{\tfrac{4n_i}{|\alpha_i|}, M_i-m_i\big\} \leq \prod_{i=1}^{k}\min\big\{\tfrac{4n_i}{|\alpha_i|}, 2M_i\big\},$$

$$\Big|\sum_{C}\psi_\alpha(c)\Big| \leq \prod_{i=1}^{k}\min\big\{\tfrac{4n_i}{|\alpha_i|}, m_i+1\big\}.$$

Thus,

$$\begin{aligned}\sum_{\alpha}\Big|\sum_{B'}\psi_\alpha(b')\Big|\Big|\sum_{C}\psi_\alpha(c)\Big| &\le \sum_{\alpha}\prod_{i=1}^{k}\min\left\{\tfrac{4n_i}{|\alpha_i|},2M_i\right\}\min\left\{\tfrac{4n_i}{|\alpha_i|},m_i+1\right\}\\ &\le \prod_{i=1}^{k}\left(\sum_{|\alpha_i|\le n_i/2}\min\left\{\tfrac{4n_i}{|\alpha_i|},2M_i\right\}\min\left\{\tfrac{4n_i}{|\alpha_i|},m_i+1\right\}\right)\\ &\le \prod_{i=1}^{k}\left(\sum_{0\le\alpha_i\le n_i/2}\min\left\{\tfrac{8n_i}{\alpha_i},4M_i\right\}\min\left\{\tfrac{4n_i}{\alpha_i},m_i+1\right\}\right),\end{aligned}$$

and the same upper bound holds for the sum in B''.

Observe that

$$\begin{aligned}\sum_{0\le\alpha_i\le n_i/2}\min\left\{\tfrac{8n_i}{\alpha_i},4M_i\right\}\min\left\{\tfrac{4n_i}{\alpha_i},m_i+1\right\} &= 4\sum_{0\le\alpha\le\frac{2n_i}{M_i}}M_i(m_i+1)\\ &+8\sum_{\frac{2n_i}{M_i}<\alpha\le\frac{4n_i}{m_i+1}}\frac{n_i(m_i+1)}{\alpha}+32\sum_{\alpha>\frac{4n_i}{m_i+1}}\frac{n_i^2}{\alpha^2}=S_1+S_2+S_3.\end{aligned}$$

To estimate the quantities S_i we use, for $2\le A<B$ the inequalities

$$\sum_{A\le\alpha\le B}\frac{1}{\alpha}\le\log(2B/A)\quad\text{ and }\quad\sum_{A<\alpha}\frac{1}{\alpha^2}\le\frac{2}{A},$$

and obtain

$$\begin{aligned}&S_1\le 4M_i(m_i+1)\left(\frac{2n_i}{M_i}+1\right)\le 12n_i(m_i+1),\\ &S_2\le 8n_i(m_i+1)\log\left(\frac{4M_i}{m_i+1}\right)\le n_i(m_i+1)\left(12+8\log\left(\frac{M_i}{m_i+1}\right)\right),\\ &S_3\le 16n_i(m_i+1).\end{aligned}$$

Thus we have,

$$S_1+S_2+S_3\le n_i(m_i+1)\left(40+8\log\left(\frac{M_i}{m_i+1}\right)\right)\tag{11}$$

and then

$$\sum_{\psi}\Big|\sum_{B'}\psi_\alpha(b')\Big|\Big|\sum_{C}\psi_\alpha(c)\Big|\le\prod_{i=1}^{k}n_i(m_i+1)\left(40+8\log\left(\frac{M_i}{m_i+1}\right)\right)$$

Combining the previous estimate we obtain the following bound for the last sum in (7)

$$\frac{|\widehat{A}|}{|G||C|}\sum_{\psi}\Big|\sum_{B'}\psi(b')\Big|\Big|\sum_{C}\psi(c)\Big| \le |\widehat{A}|\prod_{i=1}^{k}\left(40+8\log\left(\frac{M_i}{(m_i+1)}\right)\right), \tag{12}$$

since $n_1\cdot n_2\cdots n_k=|G|$ and $(m_1+1)\cdot(m_2+1)\cdots(m_k+1)=|C|$ by definition. The same bound applies to the sum in (8).

Observe that if $(x_1,\dots,x_k)\in B'\setminus B$, then $H_j+1-m_j\le x_j\le H_j$ for at least one $j\in\{1,\dots,k\}$. This implies

$$|B'|-|B|\le\sum_{i=1}^{k}\Big(m_i\prod_{j\neq i}(M_j+m_j)\Big)=\sum_{i=1}^{k}\Big(\frac{m_i}{M_i+m_i}\prod_{j=1}^{k}(M_j+m_j)\Big)\le|B|2^k\sum_{i=1}^{k}\frac{m_i}{M_i}. \tag{13}$$

Combining (7) and (8) with (12) and (13) we get

$$\left||A\cap B|-\frac{|A||B|}{|G|}\right|\le\frac{|A||B|2^k\sum_{i=1}^{k}\frac{m_i}{M_i}}{|G|}+|\widehat{A}|\prod_{i=1}^{k}\left(40+8\log\left(\frac{M_i}{(m_i+1)}\right)\right). \tag{14}$$

If $|B|>\frac{|\widehat{A}||G|}{|A|}$ we take

$$m_i=\left\lfloor M_i\frac{|\widehat{A}||G|}{|B||A|}\right\rfloor\le M_i-1,$$

and introduce it into (14) to get

$$\left||A\cap B|-\frac{|A||B|}{|G|}\right|\le|\widehat{A}|\left(k2^k+\left(40+8\log\left(\tfrac{|B||A|}{|\widehat{A}||G|}\right)\right)^k\right).$$

If $|B|\le\frac{|\widehat{A}||G|}{|A|}$ we take $m_i=M_i-1$ and then we have

$$\left||A\cap B|-\frac{|A||B|}{|G|}\right|\le|\widehat{A}|\left(k2^k+40^k\right).$$

Using the notation $\log_+ x=\max(0,\log x)$ and the crude estimate $(A+B)^k\le 2^k(A^k+B^k)$, both inequalities can be bounded by

$$\begin{aligned}\left||A\cap B|-\frac{|A||B|}{|G|}\right| &\le |\widehat{A}|\left(k2^k+\left(40+8\log_+\left(\tfrac{|B||A|}{|\widehat{A}||G|}\right)\right)^k\right)\\ &\le |\widehat{A}|\left(k2^k+2^k40^k+2^k8^k\log_+^k\left(\tfrac{|B||A|}{|\widehat{A}||G|}\right)\right)\\ &\le \theta|\widehat{A}|\left(1+\log_+^k\left(\tfrac{|B||A|}{|\widehat{A}||G|}\right)\right)\end{aligned}$$

for some $\theta<100^k$. □

3. Applications

In this section we will illustrate how Theorem 1 applies to some classical problems.

Once we are able to reduce the congruence problem to estimate the quantity $|A\cap B|$ for suitable $A, B\subset G$, we must be able to estimate $|\widehat{A}|$.

In our study, estimates for $|\widehat{A}|$ will follow from good bounds on sums of the form

$$\sum_{a\in A}\psi_\alpha(a)=\sum_{(x_1,\dots,x_n)\in A} e\left(\frac{\alpha_1x_1+\cdots+\alpha_kx_k}{p}\right),\quad A\subseteq G=\mathbb{F}_p^n, \tag{15}$$

where A may not be an algebraic variety but a more general set, and clearly Kloosterman sums are examples of this kind. But for more general finite abelian groups we will deal with sums of the form

$$\sum_{a\in A}\psi_\alpha(a)=\sum_{(x_1,\dots,x_n)\in A} e\left(\frac{\alpha_1x_1}{n_1}+\cdots+\frac{\alpha_kx_k}{n_k}\right)\quad A\subseteq G=\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}. \tag{16}$$

In both cases we will consider $\alpha=(\alpha_1,\dots,\alpha_k)\in G\setminus\{(0,\dots,0)\}$. Recall that some α_i might be zero but not all, and this would make a difference sometimes.

In some situations, good bounds for the quantities (15) and (16) rely on very deep results. That is the case of Weil's estimates for Kloosterman sums, which arised from the study of the structure of L-functions of algebraic varieties over finite fields and the so called Riemman Hypothesis for them. But sometimes these estimates are easy to obtain. That is the case of Sidon sets, which are studied later in this section.

3.1. **Dense Sidon sets.** The additive properties of Sidon sets give us good bounds for the quantity $|\widehat{A}|$. It is easy to obtain a trivial upper bound for the size of a Sidon set in G. Indeed if A is a Sidon set, then $|A-A|=|A|^2-|A|+1\leq|G|$. This gives $|A|\leq\sqrt{|G|-3/4}+1/2$ and there are examples where the equality holds.

Proposition 1. *Let $A\subset G$ be a Sidon set with $|A|\geq|G|^{1/2}-O(1)$. Then,*

$$|\widehat{A}|=O(|A|^{1/2}).$$

Proof. Note that

$$\Big|\sum_{a\in A}\psi(a)\Big|^2=\sum_{a,a'\in A}\psi(a-a')=\sum_{m\in G}r_{A-A}(m)\psi(m)=\sum_{m\in G}(r_{A-A}(m)-1)\psi(m). \tag{17}$$

Since A is a Sidon set, we have that $r_{A-A}(m)\leq 1$ for $m\neq 0$ and $r_{A-A}(0)=|A|$. It follows from (17)

$$\Big|\sum_{a\in A}\psi(a)\Big|^2=|A|-1-\sum_{m\notin A-A}\psi(m). \tag{18}$$

Thus we need to study the set $A-A$. It is clear that every pair $(a,a'),\ a,a'\in A$, uniquely determines the element $m=a-a'$, whenever $a\neq a'$, and the zero element is represented by every pair $(a,a),\ a\in A$. Therefore

$$|A-A|=|A|^2-|A|+1\geq |G|-O(|A|),$$

since $|A|\geq |G|^{1/2}-O(1)$ by hypothesis. The previous equation implies that for a given character $\psi=\psi_\alpha$, we have

$$\Big|\sum_{m\notin A-A}\psi(m)\Big|\leq |G|-|A-A|=O(|A|).$$

Combining this bound with the expression in (18), we obtain the desired result

$$|\widehat{A}|=\max_{\psi\neq\psi_0}\Big|\sum_{a\in A}\psi(a)\Big|=O\big(|A|\big)^{1/2}.$$

□

Corollary 1. *Let $A\subset G$ be a Sidon set with $|A|\geq |G|^{1/2}-O(1)$, and $B\subseteq G$ a k-dimensional box. Then*

$$|A\cap B|=\frac{|A||B|}{|G|}+O\left(|G|^{1/4}\left(1+\log_+^k\left(|B||G|^{-3/4}\right)\right)\right).$$

In particular,

$$|A\cap B|\sim\frac{|A||B|}{|G|}$$

when $\frac{|B|}{|G|^{3/4}}\to\infty$.

Proof. It follows directly from Proposition 1 and Theorem 1. □

Since the set $A=\{(x,y):\ g^x-g^y\equiv 1\pmod p\}$ is a Sidon set of $p-2$ elements in $\mathbb{Z}_{p-1}\times\mathbb{Z}_{p-1}$ (see for example [2]), we obtain the following result.

Corollary 2. *Let p be a prime number and g a primitive root in $\mathbb{F}_p^*$. The number of solutions J of the equation*

$$g^x-g^y\equiv 1\pmod p,\ x_0+1\leq x\leq x_0+M,\ y_0+1\leq y\leq y_0+M$$

is given by

$$J=\frac{M^2}{p}+O\left(p^{1/2}\left(1+\log_+^2\left(M^2p^{-3/2}\right)\right)\right).$$

Note that Corollary 2 improves the error term obtained by Garaev (6) and the one obtained by Cilleruelo.

3.2. **Parametrized curves.** If one considers the set of all points

$$A_F = \{(f_1(t), f_2(t), \dots, f_k(t)) : 1 \le t \le p\} \subset \mathbb{F}_p^k,$$

for some $F = (f_1, \dots, f_k)$ with $f_i \in \mathbb{Z}[X]$. If the polynomials f_i are linearly independent modulo p, then it follows from the Weil bounds, that

$$\sum_{a \in A_F} e\left(\frac{\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_k x_k}{p}\right) = \sum_{t=1}^{p} e\left(\frac{\alpha \cdot F(t)}{p}\right) \ll p^{1/2}, \tag{19}$$

where $\alpha \cdot F(t) = (\alpha_1, \dots, \alpha_k) \cdot (f_1(t), \dots, f_k(t)) = \alpha_1 f_1(t) + \alpha_2 f_2(t) + \cdots + \alpha_k f_k(t)$, and the constants implied deppend only on the degree of $\alpha \cdot F$.

Corollary 3. *Let p be a prime and $F = (f_1, \dots, f_k)$ with $f_i \in \mathbb{F}_p[x]$ linearly independent modulo p. For any k dimensional box $B \subseteq \mathbb{F}_p^k$*

$$|A_F \cap B| = \frac{|B|}{p^{k-1}} + O\left(p^{1/2}\left(1 + \log_+^k\left(|B| p^{1/2-k}\right)\right)\right).$$

In particular,

$$|A \cap B| \sim \frac{|B|}{p^{k-1}}$$

when $\frac{|B|}{p^{1/2-k}} \to \infty$.

Proof. The result follows from Theorem 1, Weil bounds in Equation (19) and Lang-Weil [9] results on the number of points of a variety, which states that $|A_F| = p(1 + o(1))$. □

There are many examples of this kind. For example consider an Hyperelliptic curve, given by a non-singular Weierstrass equation,

$$H_a : \quad Y^2 = X^{2g+1} + a_{2g-1} X^{2g-1} + \ldots + a_1 X + a_0,$$

where $a = (a_0, \dots, a_{2g-1}) \in \mathbb{F}_p^{2g}$.

It follows from a more general result of Lockhart [10, Proposition 1.2] that isomorphisms that preserve hyperelliptic curves given by Weierstrass equations are all of the form $(x, y) \to (t^2 x, t^{2g+1} y)$ for some $t \in \mathbb{F}_p^*$. Thus two hyperelliptic curves H_a and H_b are isomorphic if there exists $t \in \mathbb{F}_p^*$ such that

$$a_i \equiv t^{4g+2-2i} b_i \pmod{p}, \qquad i = 0, \dots, 2g-1.$$

Thus, if $F(t) = (t^{4g+2-2i} b_i)$ for $i = 0, \dots 2g-1$ then $|A_F \cap B|$ will count the number of curves which are isomorphic to H_b and whose coefficients are in B.

The standard application of the Weil bounds (see [8] for further details) gives that the number of curves which are isomorphic to a given one with coefficients in a box B is given by

$$|A_F \cap B| = \frac{|B|}{p^{2g-1}} + O\left(p^{1/2} \log^{2g} p\right),$$

and would provide an asymptotic estimate for $|A_F \cap B|$ as long as $|B|p^{-2g+1/2}\log^{-2g} p \to \infty$. It follows from Corollary 3 that

$$|A_F \cap B| = \frac{|B|}{p^{2g-1}} + O\left(p^{1/2}\left(1+\log_+^{2g}\left(|B|p^{1/2-2g}\right)\right)\right).$$

Note that our result extends the range to $|B|p^{-2g+1/2} \to \infty$, saving once again the logarithm factor.

3.3. **Plane curves.** Let us now consider sets of the form

$$A_f = \{(x_1, x_2) \,:\, f(x_1, x_2) \equiv 0 \pmod p\} \subset G = \mathbb{F}_p^2,$$

of roots of $f \in \mathbb{Z}[X_1, X_2]$ a polynomial in two variables. For these curves, Weil estimates for Kloosterman sums were generalized by Bombieri [1], who showed that, for any absolutely irreducible polynomial $f \in \mathbb{F}_p[x, y]$, of degree at most two, and any $(a, b) \neq (0, 0)$

$$\left|\sum_{a\in A_f} e\left(\tfrac{ax+by}{p}\right)\right| \ll p^{1/2}. \tag{20}$$

Observe that, in order to obtain results via Theorem 1 one should be able to estimate the number of points of A_f in first place. For example, if one considers polynomials given by $f(x, y) = x^3 + ax + b - y^2$, with nonzero discriminant, then A_f consist on the affine points of an elliptic curve and it follows from the Hasse bound that $|A_f| = p + 1 - t$ with $|t| < 2p^{1/2}$. In general, Weil and Lang [9] showed that if A is the set of affine points of any variety of dimension d

$$|A| = p^d\left(1 + o(1)\right). \tag{21}$$

Corollary 4. *Let p be a prime number, $f \in \mathbb{F}_p[x, y]$ an absolutely irreducible polynomial and $B \subseteq \mathbb{F}_p^2$ a two dimensional box. Then*

$$|A_f \cap B| = \frac{|B|}{p} + O\left(p^{1/2}\left(1+\log_+^{2}\left(|B||p|^{-3/2}\right)\right)\right).$$

In particular,

$$|A \cap B| \sim \frac{|B|}{p}$$

when $\frac{|B|}{p^{3/2}} \to \infty$.

Proof. It follows from Theorem 1, Equation (20) and Equation (21) for $d = 1$. □

3.4. **n-dimensional Hyperbolas.** Unfortunately, estimates of this kind cannot be generalized to higher dimensions. If one considers the sums

$$\sum_{a\in A_f} e\left(\frac{\alpha_1 x_1+\cdots+\alpha_k x_k}{p}\right),$$

one could not expect to obtain something like $O(p^{k/2})$ for all $\alpha\neq 0$ and a general class of polynomials for $k>2$. In this case good bounds do not follow immediately from Deligne results [3] and one should impose either more concrete geometric restrictions (see [7] for examples in $k=3$) or distinguish between different possible α's, see [4] for further discussion.

Nevertheless, in some cases this difficulty can be overpassed. Let us focus on the n-dimensional hyperbola:

$$H_n=\{(x_1,\dots,x_{n+1}) : x_1\cdots x_{n+1}\equiv 1 \pmod p\}. \tag{22}$$

In this case it is clear that non-trivial characters with zero coordinates will imply large character sums, but the number of such characters is small compared with the total number of characters.

Proposition 2. *Let p be a prime number and H_n the n-dimensional hyperbola defined by Equation (22). Then,*

$$|\widehat{H}_{n,s}|=\max_{\alpha\in X_s}\left|\sum_{a\in H_n} e\left(\frac{\alpha\cdot a}{p}\right)\right| \ll \begin{cases} p^{\frac{n}{2}} & \text{if } s=0,\\ p^{s-1} & \text{if } 1\le s\le n+1,\end{cases}$$

where X_s denotes the set of $\alpha\in\mathbb{Z}_p^{n+1}$ with exactly s zero coordinates.

Proof. The bounds for the sum in the case $s=0$ follow from the well known estimate for multilpe Kloosterman sums, which was first proved by Deligne [3]. Clearly for $s=n+1$ (that is $\alpha=(0,\dots,0)$ the sum counts the number of points in H_n, which is $(p-1)^n$.

For any $1\le s\le n$, let us consider $\alpha\in X_s$. Without loss of generality we can assume that $\alpha_1=\cdots=\alpha_s=0$ and $\alpha_i\neq 0$ for $s+1\le i\le n+1$: in particular $\alpha_{n+1}\neq 0$.

Under these asumptions we can rewrite the exponential sum as follows:

$$\sum_{a\in H_n} e\left(\frac{\alpha\cdot a}{p}\right)=\sum_{x_n=1}^{p-1}\cdots\sum_{x_1=1}^{p-1} e\left(\frac{\alpha_{s+1}x_{s+1}+\cdots+\alpha_n x_n+\alpha_{n+1}(x_1\cdots x_n)^{-1}}{p}\right).$$

Since $\alpha_{n+1}\neq 0$,

$$\sum_{x_1=1}^{p-1} e\left(\frac{\alpha_{n+1}(x_1\cdots x_n)^{-1}}{p}\right)=(-1)$$

holds for any choice of $x_1,\dots x_n$, $1\le x_i\le p-1$, and therefore

$$\sum_{x_s=1}^{p-1}\cdots\sum_{x_1=1}^{p-1} e\left(\frac{\alpha_{n+1}(x_1\cdots x_n)^{-1}}{p}\right)=\sum_{x_s=1}^{p-1}\cdots\sum_{x_2=1}^{p-1}(-1)=-(p-1)^{s-1}.$$

$$\sum_{a\in H_n} e\left(\frac{\alpha\cdot a}{p}\right) = -(p-1)^{s-1}\prod_{i=s+1}^{n}\sum_{x_i=1}^{p-1} e\left(\frac{\alpha_i x_i}{p}\right)$$
$$= (-1)^{n+1-s}(p-1)^{s-1}.$$

□

We will follow the lines of the proof of Theorem 1 to improve the error term obtained by means of classical techniques in exponential sums.

Theorem 2. *Let p be a prime and H_n be the n-dimensional hyperbola defined in* (22)*. For any cube $B\subseteq\mathbb{Z}_p^{n+1}$, of side length M, we have*

$$\left||H_n\cap B| - \frac{|B|}{p}\right| \ll p^{\frac{n}{2}}\left(1+\log_+^{n+1}\left(|B|p^{-\frac{n+2}{2}}\right)\right) + \frac{|B|^{1-\frac{1}{n+1}}}{p}\log p.$$

In particular, the asymptotic

$$|H_n\cap B| \sim \frac{|B|}{p}$$

holds as long as $|B|p^{-\frac{n+2}{2}}\to\infty$.

Proof. The proof is analogous to the one from Theorem 1, but considering a partition of all characters depending on the number of zero coordinates of them.

Recall that $B=\prod_{i=1}^{n+1}[H_i+1, H_i+M],\ 1\le M\le p$, is a cube in $\mathbb{Z}_p^{n+1}$ of side M. Consider the following approximations of B

$$B' = \prod_{i=1}^{n+1}[H_i+1-m, H_i+M], \quad B'' = \prod_{i=1}^{n+1}[H_i+1, H_i+M-m],$$

for some suitable integer $m, 0\le m\le M-1$. Denote by $C=\prod_{i=1}^{n+1}[0,m]$.

Then, it is clear that

$$|H_n\cap B| \le \frac{|B|}{p} + \frac{(|B'|-|B|)}{p} + \frac{1}{p^{n+1}|C|}\sum_{\psi\neq\psi_0}\sum_{H_n,B,C}\psi(b+c-x), \tag{23}$$

$$|H_n\cap B| \ge \frac{|B|}{p} - \frac{(|B|-|B''|)}{p} - \frac{1}{p^{n+1}|C|}\sum_{\psi\neq\psi_0}\sum_{H_n,B,C}\psi(b+c-x). \tag{24}$$

Let us focus on the estimate of (23), since the estimate for (24) is analogous.

Consider the partition of all non trivial characters indexed by the sets $X_0,\ X_1,\ \ldots,\ X_n$ defined in Proposition 2. Recall that the set X_s consists of all $\alpha\in\mathbb{Z}_p^{n+1}$ with exactly s zero coordinates.

For a fixed character ψ_α, $\alpha \in X_s$, it follows by the bounds given in (10) that

$$\left|\sum_C \psi_\alpha(c)\right| = \prod_{i=1}^{n+1}\left(\sum_{c_i=0}^{m} e\left(\frac{\alpha_i c_i}{p}\right)\right) \ll (m+1)^s \prod_{j:\,\alpha_j\neq 0} \min\left\{\tfrac{4p}{|\alpha_j|}, m+1\right\},$$

and analogously

$$\left|\sum_{B'} \psi_\alpha(b)\right| \ll M^s \prod_{j:\,\alpha_j\neq 0} \min\left\{\tfrac{4p}{|\alpha_j|}, 2M\right\}.$$

Thus, when summing up over all $\alpha \in X_s$ and using the estimates given in (11)

$$\sum_{\alpha\in X_s}\left|\sum_C \psi_\alpha(c)\right|\left|\sum_{B'} \psi_\alpha(b)\right| \ll (m+1)^{n+1} M^s p^{n+1-s}\left(1+\log^{n+1-s}\left(\frac{M}{m+1}\right)\right).$$

Taking this into account and partitioning the last sum in (23) we have

$$\left||H_n\cap B| - \frac{|B|}{p}\right| \ll \frac{|B|m}{pM} + \sum_{s=0}^{n} |\widehat{H}_{n,s}|\left(\frac{M}{p}\right)^s\left(1+\log^{n+1-s}\left(\frac{M}{m+1}\right)\right).$$

As for Theorem 1, we might choose $m = \min\left\{\left\lfloor M\frac{p^{1+\frac{n}{2}}}{|B|}\right\rfloor, M-1\right\} \leq M-1$ to minimize the error and obtain:

$$\begin{aligned}\left||H_n\cap B| - \frac{|B|}{p}\right| \ll& \sum_{s=0}^{n} |\widehat{H}_{n,s}|\left(\frac{M}{p}\right)^s\left(1+\log_+^{n+1-s}\left(|B|p^{-\frac{n+2}{2}}\right)\right)\\ \ll& p^{\frac{n}{2}}\left(1+\log_+^{n+1}\left(|B|p^{-\frac{n+2}{2}}\right)\right) + \frac{M^n}{p}\left(1+\log_+\left(|B|p^{-\frac{n+2}{2}}\right)\right)\end{aligned}$$

Which concludes the proof by noting that $|B| = M^{n+1}$. □

The classical bounds for this problem give

$$|H_n\cap B| = \frac{|B|}{p} + O\left(p^{\frac{n}{2}}\log^{n+1} p + \frac{|B|^{1-\frac{1}{n+1}}}{p}\log p\right),$$

which provides an asymptotic estimate for $|H_n\cap B|$ as long as $|B|p^{-\frac{n+2}{2}}\log^{-1} p \to \infty$.

Once again, Theorem 2 improves the classical bounds by extending the range for an asymptotic behaviour: asymptotic estimates hold for any box of size $|B|p^{-\frac{n+2}{2}} \to \infty$.

For $n \geq 4$ Shparlinski [12] obtained a better bound by exploiting multiplicative characters, but in the case $n = 2, 3$ Theorem 2 is still better that what was known.

4. Acknoledgments

This work supported by grants MTM 2011-22851 of MICINN and ICMAT Severo Ochoa project SEV 2011-0087. The second author was supported by a FPU grant Ministerio de Educación, Cultura y Deporte, Spain.

References

[1] E. Bombieri, On exponential sums in finite fields, *Amer. J. Math.* **88** (1966), 71–105.

[2] J. Cilleruelo, 'Combinatorial problems in finite fields and Sidon sets', *Combinatorica* **32** 5 (2012), 497–511.

[3] P. Deligne, *Cohomologie étale*, Lecture Notes in Mathematics, Vol. 569, Springer-Verlag, Berlin, 1977.

[4] E. Fouvry and N. Katz, A general stratification theorem for exponential sums, and applications, *J. Reine Angew. Math.*, **540** (2001), 115–166.

[5] M. Z. Garaev, 'On the logarithmic factor in error term estimates in certain additive congruence problems', *Acta Arith.*, **124** no.1 (2006), 27–39.

[6] D.R. Heath-Brown, 'Arithmetic applications of Kloosterman sums', *Nieuw Arch. Wiskd.*, **5** no.1 (2000), 380–384.

[7] C. Hooley, *On exponential sums and certain of their applications*, Number theory days, 1980 (Exeter, 1980), London Math. Soc. Lecture Note Ser., **56**, 92–122, Cambridge Univ. Press, 1982.

[8] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, 2004.

[9] S. Lang and A. Weil, 'Number of points of varieties in finite fields', *Amer. J. Math.* **76** (1954), 819–827.

[10] P. Lockhart, 'On the discriminant of a hyperelliptic curve', *Trans. Amer. Math. Soc.*, **342** (1994), 729–752.

[11] A. Weil, 'On some exponential sums', *Proc. Natl. Acad. Sci. USA*, **34** (1948), 204–207.

[12] I. E. Shparlinski, On the distribution of points on multidimensional modular hyperbolas. *Proc. Japan Acad. Ser. A Math. Sci.* **83** (2007), no. 2, 5–9.

J. Cilleruelo: Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Madrid, Spain

E-mail address: franciscojavier.cilleruelo@uam.es

A. Zumalacárregui: Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Madrid, Spain

E-mail address: ana.zumalacarregui@uam.es