AN ADDITIVE PROBLEM IN FINITE FIELDS WITH POWERS OF ELEMENTS OF LARGE MULTIPLICATIVE ORDER

JAVIER CILLERUELO AND ANA ZUMALACÁRREGUI

ABSTRACT. For a given finite field $\mathbb{F}_q$, we study sufficient conditions to guarantee that the set $\{\theta_1^x + \theta_2^y : \ 1 \le x \le M_1, \ 1 \le y \le M_2\}$ represents all the nonzero elements of $\mathbb{F}_q$. We investigate the same problem for $\theta_1^x - \theta_2^y$ and as a consequence we prove that any element in the finite field of q elements has a representation of the form $\theta^x - \theta^y$, $1 \le x, y \le \sqrt{2}q^{3/4}$ whenever θ has multiplicative order at least $\sqrt{2}q^{3/4}$. This improves the previous known bound for a question possed by A. Odlyzko.

1. INTRODUCTION

Let p be a large prime and g a primitive root modulo p. Andrew Odlyzko asked for which values of M the set

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

contains every residue class modulo p. He conjectured that one can take M to be as small as $p^{1/2+\epsilon}$, for any fixed $\epsilon > 0$ and p large enough in terms of ϵ.

Some results have been obtained in this direction. Rudnik and A. Zaharescu [5], using standard methods of characters sums, proved that one can take $M \ge cp^{3/4}\log p$ for some $c > 0$. This range was improved to $M \ge cp^{3/4}$ by M. Z. Garaev and K.-L. Kueh [2] and independently by S. V. Konyagin [4]. Later, V. C. García [3] showed that $c = 2^{5/4}$ is an admissible constant and the first author [1], using a combinatorial approach, improved the constant to $\sqrt{2} + \varepsilon$, but for p large enough in terms of $\epsilon > 0$.

In this note we exploit properties of Sidon sets, combined with the classic exponential sums techniques, to obtain new results on a generalization of the original problem of Odlyzko.

We will no longer study differences of powers of primitive roots in prime fields, but differences of elements of large multiplicative order in arbitrary finite fields $\mathbb{F}_q$. We write $\mathrm{ord}_q(\theta)$ for the multiplicative order of θ in $\mathbb{F}_q$.

Theorem 1. *Let θ be an element of $\mathbb{F}_q$. If $\min(ord_q(\theta), M) \ge \sqrt{2}q^{3/4}$, then*

$$\{\theta^x - \theta^y : \ 1 \le x, y \le M\} = \mathbb{F}_q.$$

2000 *Mathematics Subject Classification.* 11N69 (11A07 11N25) .

Key words and phrases. Primitive roots, finite fields, Sidon sets, difference sets.

The second author is supported by a FPU grant from Ministerio de Educación, Ciencia y Deporte, Spain. Both authors are supported by grants MTM 2011-22851 of MICINN and ICMAT Severo Ochoa project SEV-2011-0087.

Applying the previous result when θ is a primitive root we obtain the announced improvment on the problem of Odlyzko.

Corollary 1. *Let g be a primitive root of $\mathbb{F}_q$. If $M \geq \sqrt{2}q^{3/4}$, then*

$$\{g^x - g^y : 1 \leq x, y \leq M\} = \mathbb{F}_q.$$

One can generalize Theorem 1, by considering the set of sums of powers of two elements in the field.

Theorem 2. *Let θ_1, θ_2 be two elements of $\mathbb{F}_q$. If*

$$\min(ord_q(\theta_1), \lfloor M_1/2 \rfloor) \cdot \min(ord_q(\theta_2), \lfloor M_2/2 \rfloor) \geq q^{3/2},$$

then

$$\begin{aligned} \mathbb{F}_q^* &\subseteq \{\theta_1^x + \theta_2^y : 1 \leq x \leq M_1,\ 1 \leq y \leq M_2\}, \\ \mathbb{F}_q^* &\subseteq \{\theta_1^x - \theta_2^y : 1 \leq x \leq M_1,\ 1 \leq y \leq M_2\}. \end{aligned}$$

Let us note that, if we consider the case $\theta_1 = \theta_2$ and $M_1 = M_2 = M$ the hypothesis in Theorem 2, say $\min(\mathrm{ord}_q(\theta), M) \geq 2q^{3/4}$, are more restrictive that those in Theorem 1. The loss on the constant $\sqrt{2}/2$ in the hypothesis relies on the fact that the set $\{\theta_1^x - \theta_2^y : 1 \leq x \leq M_1, 1 \leq y \leq M_2\}$ is no longer symmetric if $\theta_1 \neq \theta_2$ or $M_1 \neq M_2$.

We observe also that 0 may not belong to these sets. If θ_1, θ_2 has order $(q-1)/2$ and q is prime, the elements $\theta_1^x + \theta_2^y$ are sum of two squares and 0 is not of this form if $q \equiv 3 \pmod 4$.

2. Preliminaries

Let G be an abelian group. We recall that a set $\mathcal{A} \subset G$ is a Sidon set if all the non zero differences $a - a',\ a, a' \in \mathcal{A}$ are distinct.

Given a set B, it is usual to denote by $r_{B-B}(m)$ to the number of representations of $m \in G$ in the form $m = b - b'$ with $b, b' \in B$. Thus, Sidon sets are those sets $\mathcal{A}$ with $r_{\mathcal{A}-\mathcal{A}}(m) \leq 1$ for all $m \neq 0$.

There are many interesting examples of Sidon sets, but we are interested in those described in the following Lemma.

Lemma 1. *Let q be a power of a prime and λ a nonzero element of $\mathbb{F}_q$. For any given g_1, g_2, primitive roots of $\mathbb{F}_q$, the sets*

$$\mathcal{A}^-(g_1, g_2, \lambda) = \{(x, y) :\ g_1^x - g_2^y = \lambda\} \tag{2}$$

$$\mathcal{A}^+(g_1, g_2, \lambda) = \{(x, y) :\ g_1^x + g_2^y = \lambda\} \tag{3}$$

are Sidon sets in $G = \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$.

This is a well known fact, see for example [1], but we include the proof for completeness.

Proof. We will first show the Sidon condition for $\mathcal{A}^-(g_1, g_2, \lambda)$, and the same argument applies to $\mathcal{A}^+(g_1, g_2, \lambda)$.

For a fixed $m = (m_1, m_2) \in G$, $m \neq 0$, we will show that if there exist $a = (x, y), a' = (x', y') \in \mathcal{A}^-(g_1, g_2, \lambda)$ for which $m = a - a'$, then they are uniquely determined by m.

Observe that $m = a - a'$ is equivalent to $x = x' + m_1$ and $y = y' + m_2$ modulo $(q-1)$, which implies that

$$g_1^x \equiv g_1^{x'+m_1} \pmod{q} \quad \text{and} \quad g_2^y \equiv g_2^{y'+m_2} \pmod{q}.$$

Combining this observation with the fact that both a and a' are in $\mathcal{A}^-(g_1, g_2, \lambda)$, we have that

$$g_2^{y'} \left(g_1^{m_1} - g_2^{m_2}\right) \equiv \lambda \left(1 - g_1^{m_1}\right). \tag{4}$$

If $m_1 \neq 0$, then y' is uniquely determined by equation (4) (and so x, x' and y). If $m_1 = 0$, equation (4) implies that $m_2 = 0$, which contradicts the assumption $m \neq 0$. □

For a real nonzero number x, let us denote by $e(x)$ the complex number $e^{2\pi i x}$. The additive characters ψ in $G = \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$ are all of the form $\psi_{r,s}(x, y) = e\left(\frac{rx+sy}{q-1}\right)$, where $0 \leq r, s \leq q-1$ and the character corresponding to $r = s = 0$ is the principal character.

Proposition 1. *For any Sidon set $\mathcal{A}$ described in Lemma 1 and for any non principal character ψ in G, we have*

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

Proof. We first consider the case (2) with $g_1 = g_2$: $\mathcal{A} = \mathcal{A}^-(g_1, g_1, \lambda)$. Note that for any nontrivial character ψ in $G = \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$ we have that

$$\Big|\sum_{a \in \mathcal{A}} \psi(a)\Big|^2 = \sum_{a, a' \in \mathcal{A}} \psi(a - a') = \sum_{m \in G} r_{\mathcal{A}-\mathcal{A}}(m)\psi(m) = \sum_{m \in G} (r_{\mathcal{A}-\mathcal{A}}(m) - 1)\psi(m). \tag{5}$$

Since $\mathcal{A}$ is a Sidon set, we have that $r_{\mathcal{A}-\mathcal{A}}(m) \leq 1$ for all $m \neq 0$ and $r_{\mathcal{A}-\mathcal{A}}(0) = |\mathcal{A}|$. It follows from (5) that

$$\Big|\sum_{a \in \mathcal{A}} \psi(a)\Big|^2 = |\mathcal{A}| - 1 - \sum_{m \notin \mathcal{A}-\mathcal{A}} \psi(m). \tag{6}$$

Thus we need to study the set $\mathcal{A} - \mathcal{A}$. Observe that the $3(q-2)$ elements of the form $(z, 0), (0, z)$ and (z, z), $1 \leq z \leq q-2$ do not belong to $\mathcal{A} - \mathcal{A}$. Indeed, if $(z, 0) = (x + z, y) - (x, y)$ for some $(x + z, y), (x, y) \in \mathcal{A}$ we would have that $g^{x+z} - g^y = g^x - g^y = \lambda$, which is impossible unless $z \equiv 0 \pmod{q-1}$. The same argument applies to the elements of the form $(0, z)$ and (z, z).

Furthermore, since $|G|-|\mathcal{A}-\mathcal{A}|=|G|-(|\mathcal{A}|^2-|\mathcal{A}|+1)=3(q-2)$, it follows that those are the only elements $m\notin\mathcal{A}-\mathcal{A}$. Therefore, for a given $\psi=\psi_{r,s}$, we have

$$\sum_{m\notin\mathcal{A}-\mathcal{A}}\psi(m)=\sum_{z=1}^{q-2}e\Big(\frac{rz}{q-1}\Big)+\sum_{z=1}^{q-2}e\Big(\frac{sz}{q-1}\Big)+\sum_{z=1}^{q-2}e\Big(\frac{(r+s)z}{q-1}\Big)\geq -3,$$

since every such sum is either -1 or $q-2$, depending on the values r and s.

Combining this bound with the expression in (6), we obtain the desired result

$$\Big|\sum_{a\in\mathcal{A}}\psi(a)\Big|\leq\big(|\mathcal{A}|+2\big)^{1/2}=q^{1/2}.$$

The case (2) for $g_1\neq g_2$ can be reduced the previous one. Given $(r,s)\neq(0,0)$ let t be the integer such that $g_1^t=g_2$. We observe that $(x,y)\in\mathcal{A}^-(g_1,g_2,\lambda)\iff(x,ty)\in\mathcal{A}^-(g_1,g_1,\lambda)$. Then, for any $a=(x,y)\in\mathcal{A}^-(g_1,g_2,\lambda)$ we have $\psi_{r,s}(x,y)=\psi_{r,st^{-1}}(x,ty)$. Thus

$$\max_{a\in\mathcal{A}^-(g_1,g_2,\lambda)}|\psi_{r,s}(a)|=\max_{a\in\mathcal{A}^-(g_1,g_1,\lambda)}|\psi_{r,st^{-1}}(a)|\leq q^{1/2}.$$

The case (3) is easier. It is clear that $(x,y)\in\mathcal{A}^+(g_1,g_2,\lambda)\iff(x,y)+(0,(q-1)/2)\in\mathcal{A}^-(g_1,g_2,\lambda)$ and that $\psi(a+(0,(q-1)/2))=\psi(a)\psi(0,(q-1/2))$. Thus

$$\max_{a\in\mathcal{A}^+(g_1,g_2,\lambda)}|\psi(a)|=\max_{a\in\mathcal{A}^-(g_1,g_1,\lambda)}|\psi(a+(0,(q-1)/2))|=\max_{a\in\mathcal{A}^-(g_1,g_1,\lambda)}|\psi(a)|\leq q^{1/2}.$$

□

As usual, for any set B we define $B+B=\{b+b':\ b,b'\in B\}$.

Proposition 2. *Let $\mathcal{A}$ be any Sidon set described in Lemma 1 and let B any subset of $\mathbb{Z}_{q-1}\times\mathbb{Z}_{q-1}$. If $(B+B)\cap\mathcal{A}=\emptyset$ then*

$$|B|<q^{3/2}-q+q^{1/2}+1/2.$$

Proof. The number of pairs $(b,b')\in B\times B$ with $b+b'\in\mathcal{A}$ is given by

$$\sum_{\psi}\sum_{b,b'\in B}\sum_{a\in\mathcal{A}}\psi(b+b'-a)=\frac{|B|^2|\mathcal{A}|}{|G|}+\frac{1}{|G|}\sum_{\psi\neq\psi_{0,0}}\sum_{a\in\mathcal{A}}\sum_{b,b'\in B}\psi(b+b'-a).$$

Since $(B+B)\cap\mathcal{A}=\emptyset$ it follows from the previous equation and Proposition 1 that

$$\begin{aligned}\frac{|B|^2|\mathcal{A}|}{|G|} &= \Big|\frac{1}{|G|}\sum_{\psi\neq\psi_{0,0}}\sum_{a\in\mathcal{A}}\psi(-a)\sum_{b,b'\in B}\psi(b+b')\Big| \\ &\leq \frac{1}{|G|}\sum_{\psi\neq\psi_{0,0}}\Big|\sum_{a\in\mathcal{A}}\psi(-a)\Big|\Big|\sum_{b\in B}\psi(b)\Big|^2 \\ &\leq \frac{q^{1/2}}{|G|}\sum_{\psi\neq\psi_{0,0}}\Big|\sum_{b\in B}\psi(b)\Big|^2 \\ &= \frac{q^{1/2}}{|G|}\left(|G||B|-|B|^2\right).\end{aligned}$$

This implies that

$$|B|\leq\frac{|G|q^{1/2}}{|A|+q^{1/2}}=\frac{(q-1)^2q^{1/2}}{q-2+q^{1/2}}<q^{3/2}-q+q^{1/2}+1/2.$$

The easiest way to check the last inequality is multiplying $q-2+q^{1/2}$ times $q^{3/2}-q+q^{1/2}+1/2$. □

3. Proofs of the results

We will prove the theorems by a direct application of Proposition 2 to appropriate sets B.

3.1. **Proof of Theorem 2.** Let us assume that there exists a fixed nonzero element λ of $\mathbb{F}_q$ with no solutions to

$$\theta_1^x+\theta_2^y=\lambda \text{ in } \mathbb{F}_q \text{ with } 1\leq x\leq M_1,\ 1\leq y\leq M_2, \tag{7}$$

where

$$\min(\mathrm{ord}_q(\theta_1),\lfloor M_1/2\rfloor)\cdot\min(\mathrm{ord}_q(\theta_2),\lfloor M_2/2\rfloor)\geq q^{3/2}. \tag{8}$$

Let us denote by $n_1=(q-1)/\mathrm{ord}_q(\theta_1)$ and let g_1 be a generator of $\mathbb{F}_q^*$ satisfying $\theta_1=g_1^{n_1}$. We define n_2 and g_2 analogously. Consider the Sidon set

$$\mathcal{A}=\mathcal{A}^+(g_1,g_2,\lambda)$$

and the set

$$B=\{(n_1x,n_2y):\ 1\leq x\leq\lfloor M_1/2\rfloor,\ 1\leq y\leq\lfloor M_2/2\rfloor\}.$$

It is clear that under the previous assumption above we have that $(B+B)\cap\mathcal{A}=\emptyset$. Then we apply Proposition 2 to this case taking into account that

$$|B|=\min(\mathrm{ord}_q(\theta_1),\lfloor M_1/2\rfloor)\min(\mathrm{ord}_q(\theta_2),\lfloor M_2/2\rfloor)<q^{3/2}-q+q^{1/2}+1/2<q^{3/2}$$

for $q\geq 2$, which contradicts (8). The same argument holds for the set of differences by fixing $\mathcal{A}=\mathcal{A}(g_1,g_2,\lambda)^-$.

3.2. **Proof of Theorem 1.** It is clear that the zero element has a representation of the desired form. Let us assume that

$$\min(\mathrm{ord}_q(\theta), M) \geq \sqrt{2} q^{3/4}$$

and that there exists a fixed nonzero element λ of $\mathbb{F}_q$ with no solutions to

$$\theta^x - \theta^y = \lambda \text{ in } \mathbb{F}_q \text{ with } 1 \leq x, y \leq M. \tag{9}$$

Let us denote by $n = (q-1)/\mathrm{ord}_q(\theta)$ and let g be a generator of $\mathbb{F}_q^*$ satisfying $\theta = g^n$. Consider the Sidon set

$$\mathcal{A} = \mathcal{A}^-(g, g, \lambda)$$

and the set $B = B_1 \cup B_2$ where

$$\begin{aligned} B_1 &= \{(nx, ny) : \ 1 \leq x, y \leq \lfloor M/2 \rfloor, \} \\ B_2 &= B_1 + (\tfrac{q-1}{2}, \tfrac{q-1}{2}). \end{aligned}$$

We claim that

$$(B+B) \cap \mathcal{A} = \emptyset. \tag{10}$$

Indeed, any element of $B+B$ is of the form

$$\left(nx + \delta \tfrac{q-1}{2}, ny + \delta \tfrac{q-1}{2}\right),$$

where $\delta \in \{0, 1\}$ and $1 \leq x, y \leq M$. If one of these elements would belong to $\mathcal{A}$, then

$$g^{nx + \delta \frac{q-1}{2}} - g^{ny + \delta \frac{q-1}{2}} = \lambda.$$

Since $g^{\frac{q-1}{2}} = -1$, then either $\theta^x - \theta^y = \lambda$ or $\theta^y - \theta^x = \lambda$ occur in $\mathbb{F}_q$, according to the value of δ. Therefore equation (9) would have a solution.

Proposition 2 and (10) imply an upper bound for $|B|$:

$$|B| < q^{3/2} - q + q^{1/2} + 1/2. \tag{11}$$

We will get now the lower bound:

$$|B| \geq q^{3/2} - \sqrt{2} q^{3/4} + 1/2. \tag{12}$$

If $M \geq \mathrm{ord}_q(\theta) = \frac{q-1}{n} > \sqrt{2} q^{3/4}$, then

$$\begin{aligned} \left\{(nx, ny) : \ 1 \leq x, y \leq \tfrac{q-1}{2n}\right\} &\subset B_1, \\ \left\{\left(nx + \tfrac{q-1}{2}, ny + \tfrac{q-1}{2}\right) : \ 1 \leq x, y \leq \tfrac{q-1}{2n}\right\} &\subset B_2. \end{aligned}$$

Since both sets on the left side are disjoint, we have that

$$|B| \geq 2 \left\lfloor \frac{q-1}{2n} \right\rfloor^2 \geq 2 \left\lfloor \frac{\mathrm{ord}_q(\theta)}{2} \right\rfloor^2$$

If $M < \mathrm{ord}_q(\theta) = \frac{q-1}{n}$, the sets B_1 and B_2 are disjoint and we have

$$|B| = 2 \left\lfloor \frac{M}{2} \right\rfloor^2$$

In both cases we have that

$$|B| \geq 2\left\lfloor \frac{\min(\mathrm{ord}_q(\theta), M)}{2} \right\rfloor^2 \geq 2\left(\frac{q^{3/4}}{\sqrt{2}} - \frac{1}{2}\right)^2 = \left(q^{3/4} - 1/\sqrt{2}\right)^2$$
$$= q^{3/2} - \sqrt{2}q^{3/4} + 1/2$$

as we wanted to show.

Next we observe that if (11) and (12) hold then

$$q < \sqrt{2}q^{3/4} + q^{1/2}.$$

This inequality does not hold for $q \geq 16$ and it proves the theorem for q in this range.

When $q < 16$, we observe that by assumption $\min(\mathrm{ord}_q(\theta), M) \geq \sqrt{2}q^{3/4} > q/2$ (since $q/2 \geq 2q^{3/4}$ implies $q \geq 64$). Suppose that $\lambda \notin D - D$ where $D = \{\theta^x : \ 1 \leq x \leq M\}$ and $|D| = \min(\mathrm{ord}_q(\theta), M) > q/2$. Then $D \cap (D + \lambda) = \emptyset$ and we have that

$$q \geq |D \cup (D + \lambda)| = 2|D| = 2 \cdot \min(\mathrm{ord}_q(\theta), M) > q,$$

which is a contradiction.

Acknowledgments. The authors would like to thank the anonymous referee for his suggestions, that improved the quality of the manuscript.

References

[1] J. Cilleruelo, 'Combinatorial problems in finite fields and Sidon sets', *Combinatorica*, **32** nº5 (2012).
[2] M. Z. Garaev and Ka-Lam Kueh, 'Distribution of special sequences modulo a large prime', *Int. J. Math. Math. Sci.*, no.50 (2003), 3189–3194.
[3] C. V. García, 'A note on an additive problem with powers of a primitive root.', *Bol. Soc. Mat. Mexicana* (3) **11** nº1 (2005), 1–4.
[4] S. V. Konyagin, *Bounds of exponential sums over subgroups and Gauss sums*, 4th Intern. Conf. Modern Problems of Number Theory and Its Applications, Moscow Lomonosov State Univ., Moscow, 2002, 86–114.
[5] Z. Rudnik and A. Zaharescu, 'The distribution of spacings between small powers of a primitive root', *Israel J. Math.*, **120** (2000), 271–287.

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