A second combinatorial proof on when $3(A.A) = \mathbb{F}_p$

April 9, 2011

1 Introduction

In the last note on this topic we saw how we could use the second moment method to show that if $A \subseteq \mathbb{F}_p^\times$ and $|A| \geq p^{4/5}$, then $3(A.A) = \mathbb{F}_p$, which is a little weaker than what Fourier methods give. The purpose of this note is to give yet another combinatorial proof along these lines by making use of a lemma due to Javier Cilleruelo on Sidon Sets (actually, the proof is just a trivial deduction from Cilleruelo's work).

Recall that a set A contained in an ambient abelian group G is said to be a Sidon Set if the only solutions to $a + b = a' + b'$, $a, b, a', b' \in A$, are the trivial ones. That is,

$$a + b = a' + b', a, b, a', b' \in A \implies \{a, b\} = \{a', b'\}.$$

In the paper *Combinatorial problems in finite fields and Sidon sets*

`http://arxiv.org/abs/1003.3576`

Javier Cilleruelo proves, among many other theorems, the following (Corollary 4.3 in the paper):

Theorem 1 *Let $X_1, X_2 \subseteq \mathbb{F}_p^\times$ and $X_3, X_4 \subseteq \mathbb{F}_p$. The number S of solutions to*

$$x_1 x_2 \ = \ x_3 + x_4, \ x_i \in X_i,$$

is

$$S \ = \ \frac{|X_1||X_2||X_3||X_4|}{p} + \theta\sqrt{|X_1||X_2||X_3||X_4|p}, \text{ where } |\theta| \leq 1 + o(1).$$

An almost immediate consequence of this result is the following:

Corollary 1 *Suppose* $p \geq 3$, $A \subseteq \mathbb{F}_p^\times$, $|A| \geq (1 + g(p))p^{3/4}$, *where* $g(p)$ *is a certain function such that* $g(x) = o(1)$. *Then for every* $a, b \in \mathbb{F}_p^\times$ *we have that*

$$A.A + a * A + b * A \;=\; \mathbb{F}_p.$$

To prove this corollary suppose that $\lambda \in \mathbb{F}_p$. Let

$$X_1 = X_2 = A \;\text{ and }\; X_3 = -\lambda - a * A,\; X_4 = -b * A.$$

Then, any solution to $x_1 x_2 - x_3 - x_4 = 0$ corresponds to a solution to

$$x_1 x_2 + a * y_1 + b * y_2 \;=\; \lambda,\; y_1, y_2 \in A.$$

And, applying the above theorem, the fact that $|A| \geq (1 + o(1))p^{3/4}$ guarantees that the number of such solutions is positive.

Note that this result is weaker than the $3(A.A) = \mathbb{F}_p$ result that Fourier methods give in that it (combinatorial) only works for when $|A| \geq (1 + o(1))p^{3/4}$, not $|A| > p^{3/4}$. But it is stronger in that if one lets $a, b \in A$ then $A + a * A + b * A \subseteq 3(A.A)$.