Combinatorial proofs that $3(A.A) = \mathbb{F}_p$

April 3, 2011

1 Introduction

In this note we will show that if $A \subseteq \mathbb{F}_p^\times$ and $|A| > p^{4/5}$ then $A.A + A.A + A.A = \mathbb{F}_p$. Perhaps the proof can be modified so that the exponent $4/5$ can be replaced with $3/4$, thereby matching what we get using Fourier methods.

2 The proof

We will use a type of "second moment method". To this end we find an exact formula for

$$E := \sum_{x_1 \in A, x_3, x_5 \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_p} (|\{x_2, x_4, x_6 \in A \ :\ x_1x_2 + x_3x_4 + x_5x_6 = x\}| - |A|^3/p)^2.$$

First, define

$$S := \sum_{x_1 \in A, x_3, x_5 \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_p} |\{x_2, x_4, x_6 \in A \ :\ x_1x_2 + x_3x_4 + x_5x_6 = x\}|^2,$$

and observe that

$$E \ =\ S\ -\ p|A|^7.$$

So, we just need to find the value for S: we have that

$$S \ =\ \sum_{x_1 \in A, x_3, x_5 \in \mathbb{F}_p} |\{x_2, x_4, x_6, x_2', x_4', x_6' \in A \ :\ x_1(x_2 - x_2') + x_3(x_4 - x_4') + x_5(x_6 - x_6') = 0\}|.$$

For given $x_1, x_2, x_3, x_4, x_6, x_2', x_4', x_6'$ with $x_6 \neq x_6'$, we have that there is a unique $x_5 \in \mathbb{F}_p$ such that

$$x_1(x_2 - x_2') + x_3(x_4 - x_4') + x_5(x_6 - x_6') \ = \ 0.$$

And if $x_6 = x_6'$ then we get a solution if and only if

$$x_1(x_2 - x_2') + x_3(x_4 - x_4') \ = \ 0.$$

(And x_5 can be any element of $\mathbb{F}_p$.)

It follows that

$$S \ = \ p|A|^6(|A|-1) + p|A| \sum_{x_1 \in A, x_3 \in \mathbb{F}_p} |\{x_2, x_2', x_4, x_4' \in A \ : \ x_1(x_2 - x_2') + x_3(x_4 - x_4') = 0\}|.$$

And now given $x_1, x_2, x_2', x_4, x_4'$, $x_4 \neq x_4'$, there is a unique $x_3 \in \mathbb{F}_p$ satisfying

$$x_1(x_2 - x_2') + x_3(x_4 - x_4') \ = \ 0.$$

It follows that

$$\begin{aligned} S \ &= \ p|A|^7 - p|A|^5 + p^2|A|^2 \sum_{x_1 \in A} |\{x_2, x_2' \in A \ : \ x_1(x_2 - x_2') = 0\}| \\ &= \ p|A|^7 - p|A|^5 + p^2|A|^4, \end{aligned}$$

where here we have used the fact that $0 \notin A$ to obtain the value of this last sum. Therefore,

$$E \ < \ p^2|A|^4.$$

Suppose now that there exists an $x \in \mathbb{F}_p$ that is not contained in $3(A.A)$. Then,

$$\sum_{x_1, x_3, x_5 \in A} (|\{x_2, x_4, x_6 \in A \ : \ x_1x_2 + x_3x_4 + x_5x_6 = x\}| - |A|^3/p)^2 \ = \ \sum_{x_1, x_3, x_5 \in A} |A|^6/p^2 \ = \ |A|^9/p^2.$$

In order for this to be less than our upper bound for E we must have that

$$|A|^9/p^2 \ < \ p^2|A|^4,$$

which implies

$$|A| < p^{4/5}.$$

So, as long as $|A| > p^{4/5}$ we will have $3(A.A) = \mathbb{F}_p$.