# HW problem about sums and products

February 23, 2011

As a consequence of a certain theorem due to Konyagin and Glibichuk it is known that if $A$ is a multiplicative subgroup of $\mathbb{F}_p$ having size $p^\delta$, and if we let $B := A \cup (-A) \cup \{0\}$ then the smallest $k$ for which $kB = B + \cdots + B = \mathbb{F}_p$ satisfies $k < 4^{1/\delta + o(1/\delta)}$. In this exercise I will walk you through an alternate proof (due to myself, and then refined by Todd Cochrane) that achieves the somewhat worse upper bound $k < 7^{1/\delta + o(1/\delta)}$.

**Step 1.** Let $B = A \cup (-A) \cup \{0\}$. Show that for any positive integers $\lambda, \ell$ we have that if

$$(\lambda + 1)\ell B \ \subseteq \frac{\ell B}{\lambda B}$$

(Here, $\ell B / \lambda B$ denotes all quotients $(b_1 + \cdots + b_\ell)/(b_1' + \cdots + b_\lambda')$, with the $b_i$'s and $b_j'$'s in $B$, and where we disallow $b_1' + \cdots + b_\lambda' = 0$.) then

$$\frac{\lambda \ell B}{\ell B} + B \ \subseteq \ \frac{\ell B}{\lambda \ell B}.$$

Using the Cauchy-Davenport inequality, conclude that

$$\text{either } \frac{\lambda \ell B}{\ell B} = \mathbb{F}_p \ \text{ or } \ \exists \theta \in (\lambda + 1)\ell B \text{ with } \theta \notin \frac{\ell B}{\lambda B}.$$

**Step 2.** And now suppose we have constructed elements $\theta_1, ..., \theta_m \in \mathbb{F}_p$ with $\theta_i \in r_i B$, such that

$$|B + \theta_1 * B + \cdots + \theta_m * B| \ = \ |B|^{m+1}.$$

In other words, all expressions $b_1 + \theta_1 b_2 + \cdots + \theta_m b_{m+1}$ are distinct as one varies over $(b_1, ..., b_{m+1}) \in B^{m+1}$. Then show how to construct $\theta_{m+1} \in r_{m+1}B$ so that either we have

$$B + \theta_1 * B + \cdots + \theta_{m+1} * B \ = \ \mathbb{F}_p,$$

or else

$$|B + \theta_1 * B + \cdots + \theta_{m+1} * B| \ = \ |B|^{m+1}.$$

A hint: if we had a "collision" where

$$b_1 + \theta_1 b_2 + \cdots + \theta_{m+1} b_{m+2} \ = \ b_1' + \theta_1 b_2' + \cdots + \theta_{m+1} b_{m+2}',$$

it would mean that

$$\frac{(b_1 - b_1') + \theta_1(b_2 - b_2') + \cdots + \theta_m(b_{m+1} - b_{m+1}')}{b_{m+2}' - b_{m+2}} \ = \ \theta_{m+1},$$

so long as that denominator is non-zero. But if we choose $\theta_{m+1}$ carefully this cannot happen (e.g. if $\theta_{m+1}$ is in $hB$ for sufficiently large $h$ the above lemma will tell you it cannot be such a quotient).

**Step 3.** When you finish, you will get

$$B + \theta_1 * B + \cdots + \theta_n * B \ = \ \mathbb{F}_p.$$

Since $A$ is a subgroup and since the $\theta_i \in r_i B$, conclude that

$$B + \theta_1 * B + \cdots + \theta_n * B \ \subseteq \ (1 + r_1 + \cdots + r_n)B,$$

and that $k < 1 + r_1 + \cdots + r_n$. Working through your values for the $r_i$'s it turns out that this gives $k < 7^{1/\delta + o(1/\delta)}$, as claimed.