Additive Combinatorics
March 30 – April 12, 2006

Combinational properties of residue sets modulio prime and Epdős–Graham problem.

A. A. Glibichuk
aanatol@mail.ru
Department of Mechanics & Mathemathics
Moscow State University
Vorobevy gory, 1, MSU Main Building
Moscow, 119992
RUSSIA

Abstract

Let A, B be subsets of a field of residues modulio prime p(we'll denote it $\mathbb{F}_p$). Consider the *sum set*

$$A + B := \{a + b\colon a \in A, b \in B\}$$

and the *product set*

$$A \cdot B := \{ab\colon a \in A, b \in B\}.$$

For given positive integer k denote

$$kA = \underbrace{A + A + \cdots + A}_{k}.$$

We will call subset A *symmetrical* if from $a \in A$ follows that $-a \in A$. Opposite, we call A *antisymmetrical* if from $a \in A$ follows that $a \notin A$.

The main problem is by subset $A \subset \mathbb{F}_p$ determine or estimate minimum k such that $kA = \mathbb{F}_p$.

I can present you these following lemmas:

Lemma 1. *If $A \subset \mathbb{F}_p$ and $B \subset \mathbb{F}_p$, such that B is symmetical subset and $|A|\,|B| > p$, then $8AB = \mathbb{F}_p$.*

Lemma 2. *If $A \subset \mathbb{F}_p$ and $B \subset \mathbb{F}_p$, such that B is antisymmetrical and $|A|\,|B| > p$, then $8AB = \mathbb{F}_p$.*

From this lemmas one can deduce series of corollaries and next theorem

Theorem 1. *For every* $\varepsilon > 0$*, for every sufficiently large prime* p *and for every residue* $a \pmod p$ *there are exist positive pairwise distinct integers* $x_1, \dots, x_N \leqslant p^\varepsilon$ *with* $N = 8 \cdot ([1/\varepsilon + \frac{1}{2}] + 1)^2$*, such that*

$$a \equiv x_1^{-1} + \dots + x_N^{-1} \pmod p.$$

Here x_i^{-1} denotes lowest positive integer such that $x_i^{-1} x_i \equiv 1 \pmod p$.

We will prove following theorem, using similar techniques:

Theorem 2. *Let* A *be subset of* $\mathbb{F}_p$ *such that multiplicative subgroup, generated by set* $A - A + A - A/A - A + A - A \setminus \{0\}$ *is all the group* $\mathbb{F}_p^*$*. Then*

$$k \underbrace{A \cdot A \cdot \dots \cdot A}_{f+1} = \mathbb{F}_p,$$

where $f = 4[\log p / 2 \log |A|] + 2$ *and* k *depends only on* $\log p / \log |A|$*.*

This result are interesting because one can deduce many corrolaries from this theorem.