Let $m \in \mathbb{N}$, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ be the set of the residues modulo m. If p is a prime, then $\mathbb{Z}_p$ is a field of order p. Let $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ be the set of invertible elements in $\mathbb{Z}_p$. For brevity, we will write $a \equiv b$ instead of $a \equiv b(\bmod p)$.

If $*$ is a binary operation in a ring $\mathcal{R}$ ($\mathbb{Z}_p$ or $\mathbb{C}$) on $\mathbb{Z}_p$, $A, B \subset \mathcal{R}$, then we denote

$$A * B = \{a * b : \, a \in A, b \in B\}.$$

P. Erdős and E. Szemerédi asked the following question.

Problem 2.9. *Is it true that for every nonempty finite $A \subset \mathbb{Z}$ and for every $\varepsilon > 0$*

$$\max(|A + A|, |AA|) \gg_\varepsilon |A|^{2-\varepsilon}?$$

They proved that for some $\alpha > 0$

$$\max(|A + A|, |AA|) \gg |A|^{1+\alpha}. \tag{2.30}$$

M. Nathanson established (2.30) for $\alpha = 1/31$. This value was being improved by K. Ford, G. Elekes. J. Solymosi proved (2.30) for $\alpha = 3/11 - \varepsilon$ with an arbitrary $\varepsilon > 0$; moreover, (2.30) is true for any nonempty finite $A \subset \mathbb{C}$.

It was naturally to ask if (2.30) holds for $\mathbb{Z}_p$, but it was clear that it could not hold in full generality: indeed, for $A = \mathbb{Z}_p$ we have $A + A = AA = A$. But it was reasonable to conjecture the validity of (2.30) for small A, say, $|A| \le p^{1/2}$.

Unfortunately no existing proofs of (2.30) for integer, real or complex numbers could be used for $\mathbb{Z}_p$. The assistance came from Algebra and Measure Theory.

G. A. Edgar and C. Miller gave a very elegant solution to an old problem by proving that a Borel subring of $\mathbb{R}$ either has Hausdorff dimension 0 or is equal to $\mathbb{R}$. Using their technique, among other deep ideas, J. Bourgain, N. Katz, and T. Tao in the beginning of 2003 proved the following.

Theorem 3.1. *For any $\delta > 0$ there exists $\varepsilon > 0$ such that for any $A \subset \mathbb{Z}_p$ with $p^\delta < |A| < p^{1-\delta}$ we have*

$$\max(|A + A|, |AA|) \gg_\delta |A|^{1+\varepsilon}. \tag{3.1}$$

Actually, it is not difficult to see from the proof that one can write

$$\max(|A + A|, |AA|) \gg |A| p^{c\delta}$$

for $p^{1/2} < |A| < p^{1-\delta}$.

In the paper of J. Bourgain and SK (3.1) was improved for small A.

Theorem 3.2. *There exists $c > 0$ such that for any nonempty $A \subset \mathbb{Z}_p$ with $|A| \le p^{1/2}$ we have*

$$\max(|A+A|, |AA|) \gg |A|^{1+c}. \tag{3.2}$$

Another, more important, result of that paper, was related to exponential sums over subgroups.

We take an arbitrary subgroup G of the group $\mathbb{Z}_p^*$. Let $t = |G|$. For $u \in \mathbb{R}$ we denote $e(u) = \exp(2\pi i u)$. The function $e(\cdot)$ is 1-periodic, and this allows us to talk about $e(a/p)$ for $a \in \mathbb{Z}_p$. We denote

$$S(a, G) = \sum_{x \in G} e(ax/p).$$

The following result has been established.

Theorem 3.3. *For any $\delta > 0$ there exists $\varepsilon > 0$ such that for any G with $|G| > p^\delta$ we have*

$$\max_{a \in \mathbb{Z}_p^*} |S(a, G)| \ll_\delta |G| p^{-\varepsilon}. \tag{3.3}$$

The proof of Theorem 3.3 uses the estimates in the sums— products problem. It suffices to use Theorem 3.1; using Theorem 3.2 gives

$$\varepsilon = \exp(-(1/\delta)^C)$$

with an absolute constant C.

Now we will discuss the proof of Theorem 3.2. Denote

$$I(A) = \{a_1(a_2 - a_3) + a_4(a_5 - a_6) : a_j \in A\}.$$

We proved the following estimates for $|I(A)|$.

Theorem 3.4. *If* $|A| > \sqrt{p}$ *then* $|I(A)| > p/2$.

Theorem 3.5. *If* $0 < |A| \leq \sqrt{p}$ *then*

$$|I(A)| \times |A - A| \gg |A|^{5/2}. \tag{3.4}$$

Take any element $a_0 \in A \cap \mathbb{Z}_p^*$. For any $b \in A - A$ we have $a_0 b \in I(A)$. Therefore, $|I(A)| \geq |A - A|$, and (3.4) implies

$$|I(A)| \gg |A|^{5/4}. \tag{3.5}$$

Now we comment how to get Theorem 3.2 from (3.5). first, observe that

$$I(A) \subset AA - AA + AA - AA,$$

and (3.5) implies

$$|AA - AA + AA - AA| \gg |A|^{5/4}. \tag{3.6}$$

Combining Lemma 2.4 and Lemma 2.2 from the paper of Bourgain, Katz, Tao, we have the following result (Katz, Tao, Nathanson, Ruzsa).

Lemma 3.6. *There exist an absolute constant $C > 0$ such that if*

$$\max(|A + A|, |AA|) \leq K|A|,$$

then there exists a set $A' \subset A$ such that

$$|A'| \geq C^{-1}K^{-C}|A|$$

and

$$|A'A' - A'A' + A'A' - A'A'| \ll CK^{C}|A'|.$$

It is easy to see from Lemma 3.6 that if we take

$$|A| \leq p^{1/2}, \quad K = \alpha |A|^{1/(5C)},$$

then

$$|A'A' - A'A' + A'A' - A'A'| \leq \beta |A'|^{5/4},$$

where β is small if α is. But the last inequality does not agree with (3.6). This shows that

$$\max(|A+A|, |AA|) \gg |A|^{1+1/(5C)},$$

if $|A| \leq p^{1/2}$.

For $\xi \in \mathbb{Z}_p$ we denote

$$S_\xi(A) := \{a + b\xi : a, b \in A\}.$$

To prove estimates for $|I(A)|$ we need some Lemmas.

Lemma 3.7. *Let $\xi \in \mathbb{Z}_p$. Then the condition*

$$|S_\xi(A)| < |A|^2 \tag{3.7}$$

is equivalent to existence of a_1, a_2, a_3, a_4 from A such that $a_2 \not\equiv a_4$ and $\xi \equiv (a_1 - a_3)/(a_4 - a_2)$.

Proof. Since the number of sums $a_1 + \xi a_2$ with $a_1, a_2 \in A$ is $|A|^2 > |S_\xi(A)|$, then (3.7) is equivalent to existence of a_1, a_2, a_3, a_4 such that $a_2 \not\equiv a_4$ and $a_1 + \xi a_2 \equiv a_3 + \xi a_4$ as required.

Lemma 3.8. *Let $\xi \in \mathbb{Z}_p$ and (3.7) hold. Then*

$$|I(A)| \geq |S_\xi(A)|.$$

Proof. By Lemma 3.7, there exist a_1, a_2, a_3, a_4 such that $a_1 - a_3 \equiv \xi(a_4 - a_2)$. Now for any $a', a'' \in A$ we get

$$(a' + \xi a'')(a_4 - a_2) \equiv a'(a_4 - a_2) + a''(a_1 - a_3) \in I(A)$$

showing that $(a_4 - a_2)S_\xi(A) \subset I(A)$.

Lemma 3.9. *For any $H \subset \mathbb{Z}_p$ there exists $\xi \in H$ such that*

$$|S_\xi(A)| \geq \frac{|A|^2|H|}{|A|^2 + |H|}.$$

Proof. Set

$$\nu_\xi(b) = |\{(a_1, a_2) : \, a_1, a_2 \in A, b \equiv a_1 + \xi a_2\}|,$$

so that, by Cauchy—Schwartz inequality,

$$|A|^4 = \left(\sum_b \nu_\xi(b)\right)^2 \leq |S_\xi(A)| \sum_b \nu_\xi^2(b).$$

Therefore,

$$|A|^4 \leq |S_\xi(A)| \times |\{(a_1, a_2, a_3, a_4) : a_1 + \xi a_2 \equiv a_3 \\ +\xi a_4\}| = |S_\xi(A)|(|A|^2 + N), \quad N = |\{(a_1, a_2, a_3, a_4) : \\ a_2 \not\equiv a_4, a_1 + \xi a_2 \equiv a_3 + \xi a_4\}|.$$

(We consider that all $a_j \in A$.) Summing up over all $\xi \in H$ and taking into account that for any $a_1, a_2, a_3, a_4 \in A$ with $a_2 \not\equiv a_4$ there exists at most one $\xi \in H$ satisfying $a_1 + \xi a_2 \equiv a_3 + \xi a_4$, we obtain

$$|A|^4|H| \leq \max_{\xi \in} |S_\xi(A)|(|A|^2|H| + |A|^4)$$

as required.

Theorem 3.4. *If* $|A| > \sqrt{p}$ *then* $|I(A)| > p/2$.

Theorem 3.4 is immediate from Lemmas 3.8 and 3.9: choose $H = \mathbb{Z}_p$ and notice that if $|A|^2 > p$ then $|S_\xi(A)| \leq p < |A|^2$ for any ξ and

$$\frac{|A|^2|H|}{|A|^2+|H|} > \frac{|A|^2 p}{2|A|^2} = p/2.$$

Estimate (3.4) from Theorem 3.5

$$|I(A)| \times |A-A| \gg |A|^{5/2} \tag{3.4}$$

was improved by A. Glibichuk.

Theorem 3.10. *If* $0 < |A| \le \sqrt{p}$ *then*

$$|I(A)| \gg |A|^{3/2}. \tag{3.8}$$

It is easy to see the gap between Theorem 3.4 and Theorem 3.5 (or 3.10): if $|A| > \sqrt{p}$ then we prove that $|I(A)| > p/2$, but if $|A|$ is close to $\sqrt{p}/2$ then we know only that $|I(A)| \gg p^{3/4}$. The proof of Theorem 3.4 can be interpreted as the using of the observation that for $|A| > \sqrt{p}$ we have $(A-A)/(A-A) = \mathbb{Z}_p$, but for smaller values of $|A|$ we do not have satisfactory lower estimates for $|(A-A)/(A-A)|$. It would be interesting to know if (3.8) can be replaced by

$$|I(A)| \gg |A|^2. \tag{3.9}$$

It is not difficult to show that (3.9) holds for $A \subset \mathbb{C}$.

To prove Theorem 3.10, we can consider that

$$A \subset \mathbb{Z}_p^*, \quad |A| \geq 2.$$

We take

$$u := 2|A|^2/(9|AA|),$$

$$R := \{s \in \mathbb{Z}_p^* : |\{(a,b) : a, b \in A, s \equiv a/b\}| \geq u\}.$$

We observe that $1 \in R$ since $u \leq 2|A|^2/(9|A|) \leq |A|$. Define G as the multiplicative subgroup of $\mathbb{Z}_p^*$ generated by R. Also, let

$$F := \frac{A - A}{A - A}, \quad H = FG.$$

Recall that

$$S_\xi(A) := \{a + b\xi : a, b \in A\}.$$

Lemma 3.11. *There exists $\xi \in H$ such that*

$$\min\left(|A|u, |A|^2|H|/(|A|^2 + |H|)\right) \leq |S_\xi(A)| < |A|^2. \tag{3.10}$$

Proof. We consider two cases.

1. Case 1: $RF \neq F$. Thus, there exist $r \in R$ and $\xi \in F$ such that $h \equiv r\xi \notin F$. Clearly, $h \in H$. By Lemma 3.7,

$$|S_h(A)| = |A|^2, \quad |S_\xi(A)| < |A|^2. \tag{3.11}$$

Thus, the elements $a+bh$, $a, b \in A$ are pairwise distinct. Denote

$$A_r = \{b \in A : b/r \in A\}.$$

We have $|A_r| \geq u$ because $r \in R$. By our supposition on h, all the sums $a + b\xi \equiv a + b(h/r) \equiv a + (b/r)h$, $a \in A$, $b \in A_r$, are distinct. Therefore, $S_\xi(A) \geq |A|u$. Taking into account (3.11) we get (3.10).

2. Case 2: $RF = F$. By definition of the group G, we conclude that $F = GF = H$. By Lemma 3.7, $|S_\xi(A)| < |A|^2$ for every $\xi \in H$, and (3.10) follows from Lemma 3.9.

Notice that

$$|A|^2|H|/(|A|^2 + |H|) \geq \min(|A|^2/2, |H|/2).$$

Thus, by Lemmas 3.9 and 3.11,

$$|I(A)| \geq |S_\xi(A)| \geq \min\big(|A|u, |A|^2|H|/(|A|^2 + |H|)\big)$$
$$\geq \min(2|A|^3/(9|AA|), |A|^2/2, |H|/2). \tag{3.12}$$

The inequality $|I(A)| \gg |A|^{3/2}$ obviously holds if $|I(A)| \geq |A|^2/2$. Next, observe that

$$AA - AA \subset I(A).$$

Indeed,

$$a_1a_2 - a_3a_4 \equiv a_1(a_2 - a_3) + a_3(a_1 - a_4) \in I(A).$$

Hence,

$$|I(A)| \geq |AA - AA| \geq |AA|.$$

Therefore, in the case $|I(A)| \geq 2|A|^3/(9|AA|)$ we again have $|I(A)| \gg |A|^{3/2}$. It remains to settle the case $|I(A)| \geq |H|/2$. So, it is enough to prove that

$$|H| \gg |A|^{3/2}. \tag{3.13}$$

Lemma 3.12. *There is a coset G_1 of G such that*

$$|A \cap G_1| \geq |A|/3. \tag{3.14}$$

Proof. Assume the contrary. Let $A_1, A_2, \ldots$ be the nonempty intersections of A with cosets of G. Take a minimal k so that

$$\left|\bigcup_{i=1}^{k} A_i\right| > |A|/3$$

and denote

$$A' = \bigcup_{i=1}^{k} A_i, \quad A'' = A \setminus A'.$$

We have $|A'| > |A|/3$. On the other hand,

$$|A'| \leq \left|\bigcup_{i=1}^{k-1} A_i\right| + |A_k| < 2|A|/3.$$

Hence, $|A|/3 < |A'| < 2|A|/3$ and

$$|A'| \times |A''| = |A'|(|A| - |A'|) > 2|A|^2/9. \tag{3.15}$$

Denote for $s \in \mathbb{Z}_p^*$

$$f(s) := \{(a,b) : a \in A',\, b \in A'', a/b \equiv s\}.$$

Note that if $a \in A'$, $b \in A''$, then $a/b \notin G$ and, therefore, $a/b \notin R$. Hence, for any s we have the inequality $f(s) < 2|A|^2/(9|A \cdot A|)$. Thus,

$$\sum_{s\in F^*} f(s)^2 \le \frac{2|A|^2}{9|AA|} \sum_{s\in F^*} f(s)$$

$$= \frac{2|A|^2|A'| \times |A''|}{9|AA|}. \tag{3.16}$$

Denote for $s \in \mathbb{Z}_p^*$

$$g(s) := \{(a,b) : a \in A',\, b \in A'', ab \equiv s\}.$$

By Cauchy—Schwartz inequality,

$$\left(\sum_{s\in F} g(s)\right)^2 \le |AA| \sum_{s\in F} g(s)^2.$$

Therefore,

$$\sum_{s\in F^*} g(s)^2 \geq \left(\sum_{s\in F} g(s)\right)^2 /|AA|$$

$$= \frac{(|A'|\times|A''|)^2}{|AA|}. \tag{3.17}$$

Now observe that both the sums $\sum_{s\in F^*} f(s)^2$ and $\sum_{s\in F^*} g(s)^2$ are equal to the number of solutions to the congruence $a_1'a_1'' \equiv a_2'a_2''$, $a_1', a_2' \in A'$, $a_1'', a_2'' \in A''$. Thus, comparing (3.16)

$$\sum_{s\in F^*} f(s)^2 \leq \frac{2|A|^2|A'|\times|A''|}{9|AA|} \tag{3.16}$$

and (3.17) we get

$$|A'|\times|A''| \leq 2|A|^2/9.$$

But the last inequality does not agree with (3.15), and the proof is complete.

We take a coset G_1 of G in accordance with Lemma 3.12. Fix an arbitrary $g_1 \in G_1$. Let

$$B := \{b \in G : \ g_1 b \in A\}.$$

We have

$$g_1 B = A \cap G_1, \quad |B| = |A \cap G_1| \geq |A|/3.$$

Now we use the supposition $|A| \leq \sqrt{p}$ and Corollary 2.7.

Corollary 2.7. *Let $B \subset G$ and $0 < |B| \leq p^{1/2}$. Then*

$$|G(B - B)| \gg |B|^{3/2}. \tag{2.20}$$

Therefore,

$$|G(B - B)| \gg |A|^{3/2}. \tag{3.18}$$

Fixing distinct $a_1, a_2 \in A$, we have

$$|G(B - B)| = |G(A \cap G_1 - A \cap G_1)| \leq |G(A - A)|$$
$$= |G(A - A)/(a_1 - a_2)| \leq |G(A - A)/(A - A)| = |H|.$$

So, using (3.18), we get

$$|H| \gg |A|^{3/2}, \tag{3.13}$$

and this completes the proof of Theorem 3.10.

Now let us turn to estimates for exponential sums.

Theorem 3.3. *For any $\delta > 0$ there exists $\varepsilon > 0$ such that for any G with $|G| > p^\delta$ we have*

$$\max_{a\in\mathbb{Z}_p^*} |S(a,G)| \ll_\delta |G|p^{-\varepsilon}. \tag{3.3}$$

As the proof is quite long and technical, I can give only a very short sketch now.

Recall, that by $T_k(G)$ we denote the number of solutions to the congruence

$$x_1+\cdots+x_k \equiv y_1+\cdots+y_k, \quad x_1,\ldots,x_k,y_1,\ldots,y_k \in G.$$

Our aim is to show that the following inequality holds for some $k \le k(\delta)$ and $C = C(\delta)$:

$$T_k(G) \le C|G|^{2k}p^{-0.6}. \tag{3.19}$$

We have seen that for large p one can deduce (3.13) from (3.19) sums using the inequality

$$\forall a \in \mathbb{Z}_p^* \quad \left|\sum_{x\in G} e(ax/p)\right| \le (pT_k(G)^2)^{1/2k^2}|G|^{1-2/k}.$$

Of course, the number 0.6 in (3.19) can be replaced by any number greater than 1/2.

The main part of the proof is the following Lemma.

Lemma 3.13. *There exists an absolute positive constant β satisfying the following property: for some $C = C(\delta)$ and any $k \ge k(\delta)$ there exists $k' \le k^3$ such that*

$$T_{k'}(G)|G|^{-2k'} \le (T_k(G)|G|^{-2k})^{1+\beta}$$

or

$$T_{k'}(G) \le C|G|^{2k'}p^{-0.6}.$$

Starting with some $k_0 \ge k(\delta)$, using the trivial inequality

$$T_{k_0}(G)/|G|^{2k_0} \le |G|^{-1}$$

and iterating Claim 1 we get (3.19) for $k \le k(\delta)$ with some computable $k(\delta)$.

For the proof of Lemma 3.13, we take k' as the largest power of 2 not exceeding k^3. Denote

$$\rho = T_k(G)|G|^{-2k}$$

and assume that
(3.20)
$$T_{k'}(G)|G|^{-2k'} > \rho^{1+\beta}, \quad T_{k'}(G)|G|^{-2k'} > cp^{-0.6}.$$

Our aim is to show that for some $\beta > 0$ (3.20) cannot hold for large p, and this will prove Lemma 3.13.

Denote

$$A = \left\{ a \in \mathbb{Z}_p : \left| \sum_{x \in G} e(ax/p) \right| \geq |G| p^{-1/k^3} \right\}.$$

Using (3.20), it is easy to show that

$$|A| + 1 > p\rho^{1+\beta}, \quad |A| + 1 > p^{0.4}.$$

For an even positive integer k and $y \in \mathbb{Z}_p$ let $B_k(G, y)$ be the number of solutions to the congruence

$$x_1 - x_2 + \cdots + x_{k-1} - x_k \equiv y, \quad x_1, \ldots, x_k \in G.$$

Now observe that

$$\begin{aligned}
&\left|\sum_{x\in G} e(ax/p)\right|^k \\
&= \left(\sum_{x\in G} e(ax/p)\right)^{k/2}\left(\sum_{x\in G} e(-ax/p)\right)^{k/2} \\
&= \sum_{x_1,\ldots,x_k\in G} e\left(a(x_1 - x_2 + \cdots + x_{k-1} - x_k)/p\right) \\
&= \sum_y B_k(G,y)e(ay/p).
\end{aligned}$$

Hence, for any $a \in A$ we have

$$\sum_y B_k(G,y)e(ay/p) \geq |G|^k p^{-1/k^2}. \tag{3.21}$$

This is close to the trivial upper bound

$$\sum_y B_k(G,y)e(ay/p) \leq \sum_y B_k(G,y) = |G|^k.$$

By ω we denote any function on p satisfying inequality $\omega \gg p^{-C/k^2}$; we allow ω and C to change line to line.

We can choose sets Y_1, $A_1 \subset A$ so that for $Y' = Y_1$, $A' = A_1$

$$|A'| \geq \omega |A|, \tag{3.22}$$

(3.23)

$$\left| \sum_{y \in Y'} B_k(G, y) e(ay/p) \right| \geq U := \omega |G|^k \quad (a \in A'),$$

$$\min_{y \in Y'} B_k(G, y) \leq \max_{y \in Y'} B_k(G, y)/2. \tag{3.24}$$

Let us say that Y' is GOOD, if conditions (3.22)—(3.24) are satisfied for some A'. So, Y_1 is GOOD. Moreover, we shall say that Y' is HEREDITARILY GOOD if for any $Y'' \subset Y'$ we have

$$\left| \left\{ a \in A' : \left| \sum_{y \in Y"} B_k(G, y) e(ay/p) \right| \geq \frac{|Y''|}{2|Y'|} U \right\} \right|$$
$$\geq \frac{|Y''|}{|Y'|} |A'|.$$

Both sets Y', Y'' are supposed to be invariant under multiplication by G and -1.

We do not claim that Y_1 is HEREDITARILY GOOD. But it is not difficult to show that Y_1 contains a HEREDITARILY GOOD subset Y_2 ($|Y_2| \geq \omega |Y_1|$). Denote

$$A_2 = \left\{ a \in A_1 : \left| \sum_{y \in Y_1} B_k(G, y) e(ay/p) \right| \geq \frac{|Y_2|}{2|Y_1|} U \right\}.$$

So, for all $a \in A_2$ we have

$$\left| \sum_{y \in Y_1} B_k(G, y) e(ay/p) \right| \geq \frac{|Y_2|}{2|Y_1|} U. \tag{3.25}$$

Next step in the proof is to deduce from (3.25) that, if k is a power of 2, then

$$\sum_{x_1, \ldots, x_k \in G} \sum_{y \in Y_2} B_k(G, y) e(a(x_1 - x_2 + \cdots - x_k) y/p)$$
$$\geq |G|^k V \left(\frac{\sum_{y \in Y_2} B_k(G, y) e(axy/p)}{V} \right)^k,$$

where $V = \sum_{y \in Y_2} B_k(G, y)$.

The last inequality implies

$$\sum_{x\in\mathbb{Z}_p}\sum_{y\in Y_2} B_k(G,x)B_k(G,y)e(axy/p) \geq U'|H|^{2k}$$

for all $a \in A_2$, where

$$U' = p^{-C/k}.$$

Similarly to the choice of Y_1 one can choose X_1, $A_3 \subset A_2$ so that

$$|A_3| \geq \omega|A_1|,$$

$$\left|\sum_{x\in X_1}\sum_{y\in Y_2} B_k(G,x)B_k(G,y)e(axy/p)\right| \geq \omega U'|H|^{2k} \quad (a \in A_3), \tag{3.26}$$

$$\min_{x\in X_1} B_k(G,x) \leq \max_{x\in X_1} B_k(G,x)/2.$$

Setting $z = xy$ we can rewrite the left-hand side of (3.26) as

$$\left|\sum_{z\in\mathbb{Z}_p} P(z)e(az/p)\right|,$$

where

$$P(z) = \sum_{\substack{z=xy,\\ x\in X_1, y\in Y_2}} B_k(G,x)B_k(G,y).$$

Using (3.26) and the identity

$$p\sum_{z\in\mathbb{Z}_p}(P(z))^2 = \sum_{a\in\mathbb{Z}_p}\left|\sum_{z\in\mathbb{Z}_p} P(z)e(az/p)\right|^2,$$

we can estimate $\sum_{z\in\mathbb{Z}_p}(P(z))^2$ from below; this gives a lower bound for the number of the solutions to the congruence

$$x_1y_1 \equiv x_2y_2, \quad x_1, x_2 \in X_1,\ y_1, y_2 \in Y_2.$$

This, in turn, implies the estimate for the number N of the solutions to the congruence

$$y_1y_2 \equiv y_3y_4, \quad y_j \in Y_2. \tag{3.27}$$

We show that

$$N \geq \rho^{2\beta} p^{-C/k} |Y_3|^3.$$

Recall that

$$\rho = T_k(G)|G|^{-2k}$$

and β is a small fixed positive number.

Now we can use the Balog—Szemeredi—Gowers theorem claiming that there is a subset $Y_3 \subset Y_2$ such that

$$|Y_3| \geq \left(N|Y_2|^{-3}\right)^{C_1} |Y_2|,$$

$$|Y_3 Y_3| \leq \left(N|Y_2|^{-3}\right)^{-C_1} |Y_3|.$$

At this point we use that the set Y_2 is HEREDITARILY GOOD: there is a large $A_4 \subset A_2$ such that all the sums

$$\left| \sum_{y \in Y_3} B_k(G, y) e(ay/p) \right|, \quad a \in A_4,$$

are large. This implies a lower estimate for the number of the solutions to the congruence

$$y_1 + y_2 \equiv y_3 + y_4, \quad y_j \in Y_3.$$

Using the Balog—Szemeredi—Gowers theorem again we get the existence of a large set $Y_4 \subset Y_3$ such that $Y_4 + Y_4$ is small. Also, observing that

$$|Y_4Y_4| \leq |Y_3Y_3|,$$

we conclude that both the sets $Y_4 + Y_4$, Y_4Y_4 are small. But for a small β this does not agree with the sums–products theorem asserting that

$$\max(|A + A|, |AA|) \gg |A|^{1+c} \tag{3.2}$$

provided that $|A| \leq p^{2/3}$ (it is not difficult to check that $|Y_1| \leq p^{2/3}$; hence we can use (3.2) for $A = Y_4 \subset Y_1$).

So, we see that additive properties of subgroups of $\mathbb{Z}_p^*$ help us to prove sums– products estimates for arbitrary subsets of $\mathbb{Z}_p$; conversely, sums– products estimates imply advanced additive properties of subgroups and estimates for exponential sums over subgroups.

Recently J. Bourgain has proved estimates for exponential sums over sets from a much wider class than groups.

Theorem 3.14. *For all* $Q \in \mathbb{N}$, *there is* $\tau > 0$ *and* $k \in \mathbb{N}$ *with the following property.*
Let $H \subset \mathbb{Z}_p^*$ *satisfy*

$$|HH| < |H|^{1+\tau}.$$

Then

$$\frac{1}{p}\sum_{a\in\mathbb{Z}_p}\left|\sum_{x\in H} e(ax/p)\right|^{2k}$$
$$< |H|^{2k}\left(C_Q|H|^{-Q} + p^{-1+1/Q}\right).$$

Sometimes Theorem 3.14 implies uniform estimated for $\sum_{x\in H} e(ax/p)$. Theorem 3.3 can be generalized to the following.

Theorem 3.15. *For any* $\delta > 0$ *there exists* $\varepsilon > 0$ *such that for any* $g \in \mathbb{Z}_p^*$ *and any* T *with* $T > p^\delta$ *if the elements* g^j, $0 \le j < T$, *are distinct, then*

$$\max_{a\in\mathbb{Z}_p^*}\left|\sum_{j=0}^{T-1} e(ag^j/p)\right| \ll_\delta Tp^{-\varepsilon}.$$