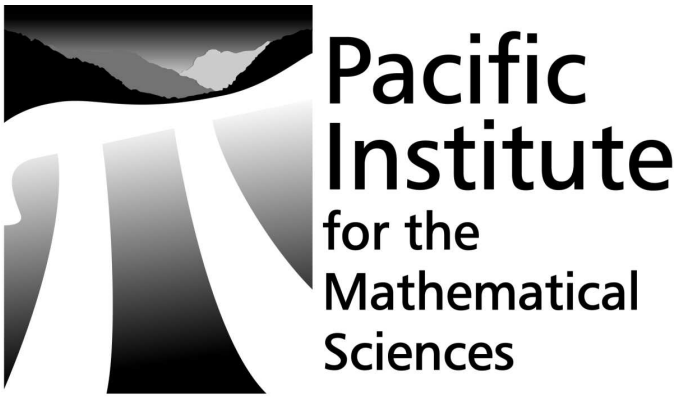

PIMS Distinguished Chair Lectures

SERGEI KONYAGIN
Moscow State University

PIMS Distinguished Chair
University of British Columbia
March–May, 2004

Exponential Sums over Multiplicative Groups in Fields of Prime Order and Related Combinatiorial Problems and Set Systems

Lecture 1

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 $\mathbb{Z}_p$. We take an arbitrary subgroup G of the group $\mathbb{Z}_p^*$. Let $t = |G|$. For brevity, we will write $a \equiv b$ instead of $a \equiv b (\mathrm{mod} p)$.

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 $a \in \mathbb{Z}_p$.

The main subject of my talks is the estimation of exponential sums over G:

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

There are some equivalent and related problems.

1. **Exponential sums with exponential functions**. Let $g \in \mathbb{Z}_p^*$ and $ord_p(g) = t$, namely

$$t = \{\min\{k > 0 : g^k \equiv 1\}\}.$$

For $a \in \mathbb{Z}_p$ we consider

$$S(a, g) = \sum_{k=0}^{t-1} e(ag^k/p).$$

Let G be the group generated by g. We have

$$G = \{g^k : k = 0, \ldots, t-1\}.$$

Hence,

$$S(a, g) = S(a, G).$$

Conversely, if G is an arbitrary subgroup of $\mathbb{Z}_p^*$ then G is generated by some $g \in \mathbb{Z}_p^*$ as a subgroup of a cyclic group $\mathbb{Z}_p^*$, and we can consider an exponential sum over G as an exponential sum with an exponential function.

2. **Gaussian sums**. Let $n \in \mathbb{N}$, $m \in \mathbb{N}$, $a \in \mathbb{Z}_m$. Consider the sum

$$S_n(a,m) = \sum_{x \in \mathbb{Z}_m} e(ax^n/m).$$

Clearly, $S_n(0,m) = m$. The simplest case is $n = 1$. For $a \in \mathbb{Z}_m \setminus \{0\}$ we have

$$S_1(a,m) = \sum_{x=0}^{m-1} e(ax/m) = \frac{e(ma/m) - e(0)}{e(a/m) - 1} = 0.$$

Thus, we have

$$\sum_{x \in \mathbb{Z}_m} e(ax/m) = \begin{cases} m, \ a = 0, \\ 0, \ a \in \mathbb{Z}_m \setminus \{0\}. \end{cases}$$

This simple property is a basic tool for using exponential sums in study of different problems modulo m.

K. Gauss evaluated $S_2(a,m)$ and, in particular, proved that $|S_2(a,p)| = \sqrt{p}$ for $a \in \mathbb{Z}_p^*$. Sometimes $S_n(a,m)$ are called Gaussian sums.

For arbitrary $n \in \mathbb{N}$ denote $d = \gcd(n, p-1)$, $t = (p-1)/d$. Consider the congruence

$$x^n \equiv 1. \tag{1.1}$$

Let g_0 be a primitive root modulo p. If $x = g_0^u$, $0 \leq u < p-1$, then (1.1) is equivalent to the congruence

$$nu \equiv 0(\mathrm{mod}(p-1)),$$

or

$$u \equiv 0(\mathrm{mod}t). \tag{1.2}$$

The number of u, $0 \leq u < p-1$, satisfying (1.2), is $(p-1)/t = d$. Therefore, for every $y \in \mathbb{Z}_p^*$ the congruence

$$x^n \equiv y$$

either does not have solutions or has d solutions. It is easy to see that $G = \{x^n : x \in \mathbb{Z}_p^*\}$ is a subgroup of $\mathbb{Z}_p^*$ and $|G| = t$.

Now we can write $S_n(a)$ as follows

$$S_n(a) = 1 + \sum_{x \in \mathbb{Z}_p^*} e(ax^n/p)$$

$$= 1 + \sum_{y \in \mathbb{Z}_p^*} e(ay/p) |\{x \in \mathbb{Z}_p^* : \, x^n \equiv y\}|$$

$$= 1 + \sum_{y \in G} de(ax/p) = 1 + \frac{p-1}{t} S(a, G).$$

We can estimate $S(a, G)$ trivially:

$$|S(a, G)| \leq \sum_{x \in G} |e(ax/p)| = \sum_{x \in G} 1 = |G|. \tag{1.3}$$

This estimate corresponds to a trivial estimate for Gaussian sums

$$|S_n(a)| \leq p.$$

Clearly, inequality (1.3) is equality if $a = 0$. We are interested in obtaining nontrivial estimates for $S(a, G)$:

$$S(a, G) = o(|G|) \quad (p \to \infty, a \in \mathbb{Z}_p^*) \tag{1.4}$$

or, for some $\delta > 0$.

$$S(a, G) \ll |G| p^{-\delta} \quad (a \in \mathbb{Z}_p^*). \tag{1.5}$$

Recall that $U \ll V$ means $|U| \le CV$ where $C > 0$ may be an absolute constant or depend on some specified parameters. Of course, in (1.4) and (1.5) we assume that a pair (p, G) belongs to some set of pairs. Trivially, (1.4) does not hold in general. If $|G| = 1$, then for any $a \in \mathbb{Z}_p$ we have $|S(a, G)| = 1$. If $p > 2$, $|G| = 2$, that is, $G = \{1, -1\}$, then

$$S(1, G) = e(1/p) + e(-1/p) = 2\cos(2\pi/p)$$
$$= |G| + O(p^{-2}).$$

We can expect that (1.4) or (1.5) holds if $|G|$ is not too small comparatively to p.

If $\max_{a\in\mathbb{Z}_p^*}|S(a,G)|$ is small comparatively to $t=|G|$, then we can deduce that for any $a\in\mathbb{Z}_p^*$ the fractional parts $\{ax/p\}$, $x\in G$, are well-distributed on $[0,1)$. To formulate this precisely, let us take an arbitrary real sequence $\{u_1,\dots,u_t\}$ and define its discrepancy as

$$D=D_t(u_1,\dots,u_t)$$
$$=\sup_{0\le\alpha<\beta\le1}\left|\frac{A([\alpha,\beta);t)}{t}-(\beta-\alpha)\right|,$$

where $A([\alpha,\beta);t)=|\{j:\{u_j\}\in[\alpha,\beta)\}|$. Thus, D is small if the distribution of the sequence $\{u_1,\dots,u_t\}$ is close to the uniform one. The theorem of Erdős and Turan asserts that for any $n\in\mathbb{N}$

$$D\le\frac{6}{m+1}+\frac{4}{\pi}\sum_{h=1}^{m}\left(\frac{1}{h}-\frac{1}{m+1}\right)\left|\frac{1}{t}\sum_{j=1}^{t}e(hu_j)\right|.$$

Take $a_0\in\mathbb{Z}_p^*$ and $\{u_1,\dots,u_t\}=\{a_0x/p:\ x\in G\}$. Then the last inequality can be written as

$$D\le\frac{6}{m+1}+\frac{4}{\pi t}\sum_{h=1}^{m}\left(\frac{1}{h}-\frac{1}{m+1}\right)|S(a_0h,G)|.$$

Therefore, if $m < p$, then

$$D \ll \frac{1}{m} + \log(m+1) \max_{a \in \mathbb{Z}_p^*} |S(a,G)|/t. \tag{1.6}$$

Assume that for some $\eta \in [1/p, 1]$ we have the estimate

$$\max_{a \in \mathbb{Z}_p^*} |S(a,G)|/t \le \eta. \tag{1.7}$$

Then, taking

$$m = \left[\frac{\eta^{-1}}{\log(\eta^{-1}) + 1} \right],$$

we deduce from (1.6)

$$D \ll \eta(\log(\eta^{-1}) + 1). \tag{1.8}$$

In particular,

$$S(a,G) = o(|G|) \quad (p \to \infty, a \in \mathbb{Z}_p^*) \tag{1.4}$$

implies

$$D \to 0 \quad (p \to \infty).$$

From the definition of the discrepancy we see that if $0 \le \alpha < \beta \le 1$ and $\beta - \alpha > D_t(u_1, \dots, u_t)$ then $[\alpha, \beta) \cap \{u_1, \dots, u_t\} \ne \emptyset$. In our case $\{u_1, \dots, u_t\} = \{a_0 x/p : x \in G\}$ we get from (1.8) under supposition (1.7) that there is an absolute constant $C > 0$ such that for $h \in \mathbb{N}$, $h \ge C\eta(\log(\eta^{-1}) + 1)p$, $n \in \mathbb{Z}$, and $a_0 \in \mathbb{Z}_p^*$ the congruence

$$n + j \equiv a_0 x, x \in G, |j| \le h, \tag{1.9}$$

has at least one solution. For small η this holds under weaker restrictions on h.

Proposition 1.1. *Assume that (1.7) holds, $h \in \mathbb{N}$, $h = [\eta p/(1+\eta)]$, $n \in \mathbb{Z}$, and $a_0 \in \mathbb{Z}_p^*$. Then (1.9) has at least one solution.*

Thus, Proposition 1.1 asserts that if exponential sums over G are small then $a_0 G$ does not produce large gaps. To prove of Proposition 1.1 we use the following Lemma.

Lemma 1.2. *Let $X \subset \mathbb{Z}_p$. Then*

$$\sum_{a \in \mathbb{Z}_p} \left| \sum_{x \in X} e(ax/p) \right|^2 = p|X|.$$

Proof of Lemma 1.2. We have

$$\begin{aligned}
&\sum_{a\in\mathbb{Z}_p}\left|\sum_{x\in X} e(ax/p)\right|^2 \\
&= \sum_{a\in\mathbb{Z}_p}\sum_{x\in X} e(ax/p)\sum_{x\in X} e(-ax/p) \\
&= \sum_{a\in\mathbb{Z}_p}\sum_{x_1\in X} e(ax_1/p)\sum_{x_2\in X} e(-ax_2/p) \\
&= \sum_{a\in\mathbb{Z}_p}\sum_{x_1,x_2\in X} e(a(x_1-x_2)/p) \\
&= \sum_{x_1,x_2\in X}\sum_{a\in\mathbb{Z}_p} e(a(x_1-x_2)/p) \\
&= \sum_{x_1=x_2\in X} p = p|X|,
\end{aligned}$$

as required.

In fact, we can treat

$$\{\sum_{x\in X} e(ax/p)\}_{a\in\mathbb{Z}_p}$$

as the Fourier transform of the characteristic function of the set X, and Lemma 1.2 is merely Parseval's identity.

Proposition 1.1. *Assume that (1.7) holds,* $h \in \mathbb{N}$, $h = [\eta p/(1+\eta)]$, $n \in \mathbb{Z}$, *and* $a_0 \in \mathbb{Z}_p^*$. *Then the congruence*

$$n + j \equiv a_0 x, x \in G, |j| \le h, \tag{1.9}$$

has at least one solution.

Proof of Proposition 1.1. Assume that congruence (1.9) is unsolvable. Then

$$0 = \sum_{x \in G} \sum_{u,v=0}^{h} \sum_{a \in \mathbb{Z}_p^*} e(a(a_0 x - n - u + v)/p).$$

Changing the order of summation, separating the term $t(h+1)^2$ corresponding to $a = 0$, and using (1.7) we get

$$t(h+1)^2 \le \sum_{a \in \mathbb{Z}_p^*} \left| \sum_{x \in G} \sum_{u,v=0}^{h} e(a(a_0 x - n - u + v)/p) \right|$$

$$= \sum_{a \in \mathbb{Z}_p^*} \left| \sum_{x \in G} e(a a_0 x/p) \right| \left| \sum_{u=0}^{h} e(au/p) \right|^2$$

$$\le \eta t \sum_{a \in \mathbb{Z}_p^*} \left| \sum_{u=0}^{h} e(au/p) \right|^2 . \tag{1.10}$$

Next, by Lemma 1.2,

$$\sum_{a\in\mathbb{Z}_p^*}\left|\sum_{u=0}^{h} e(au/p)\right|^2$$

$$=\sum_{a\in\mathbb{Z}_p}\left|\sum_{u=0}^{h} e(au/p)\right|^2-(h+1)^2$$

$$=p(h+1)-(h+1)^2.$$

After substitution of this equality into inequality (1.10) we get

$$t(h+1)^2\le\eta t\left(p(h+1)-(h+1)^2\right),$$

or, equivalently,

$$1\le\eta\left(\frac{p}{h+1}-1\right),$$

$$h+1\le\eta p/(1+\eta).$$

But this does not agree with the choice of h ($h=[\eta p/(1+\eta)]$). This completes the proof of the proposition.

Exponential sums over subgroups can be applied to the study of $1/p$-pseudo-random generators of Blum, Blum, and Shub. Let $g \geq 2$ be an integer. We consider the g-ary expansion of $1/p$. If g is fixed then we can expect (and this is true indeed) that for many primes p there is no large correlation among close digits in this expansion, and we can talk about a pseudo-random generator. Let G be the subgroup of $\mathbb{Z}_p^*$ generated by g, $t = |G|$. It is easy to see that t is the (least) period of the g-ary expansion of $1/p$. We are interested in appearances of a sequence $(d_1, \ldots, d_k)$ of g-ary digits in the expansion. Denote by σ_j, $0 \leq \sigma_j \leq g-1$, the g-ary digits of $1/p$:

$$\frac{1}{p} = \sum_{j=1}^{\infty} \sigma_j g^{-j}.$$

We observe that, for j and any g-ary string we have $\sigma_{j+i} = d_i$ for all $i = 1, \ldots, k$, if and only if

$$\frac{E}{g^k} \leq \left\{ \frac{g^j}{p} \right\} < \frac{E+1}{g^k}, \tag{1.11}$$

where $E = d_1 g^{k-1} + d_2 g^{k-2} + \cdots + d_k$.

Solvability of inequalities (1.11) both together is equivalent to solvability of the congruence $y \equiv x \in G$ for some y from the interval

$$\frac{Ep}{g^k} \le y < \frac{(E+1)p}{g^k},$$

which follows from the solvability of the congruence

$$n + j \equiv x, x \in G, |j| \le h,$$

where

$$n = \left[\frac{(2E+1)p}{2g^k}\right], \quad h = \left[\frac{p}{2g^k} - 1\right].$$

By Proposition 1.1, this congruence is solvable if

$$\max_{a \in \mathbb{Z}_p^*} |S(a, G)|/t \le \eta \tag{1.7}$$

and

$$\frac{p}{2g^k} - 1 \ge \eta p/(1+\eta).$$

So, the g-ary expansion of $1/p$ contains any string of length k if $k \le c \log(1/\eta)/\log g$ for some absolute constant $c > 0$.

Moreover, we can estimate the number $N_p(d_1, \ldots, d_k)$ of appearances of the string $(d_1, \ldots, d_k)$ in the period of the g-ary expansion of $1/p$ in terms of the discrepancy D of the set $\{x/p : x \in G\}$. Observe that

$$N_p(d_1, \ldots, d_k) = \left| \left\{ x \in G : \frac{E}{g^k} \leq \{x/p\} < \frac{(E+1)}{g^k} \right\} \right|.$$

By the definition of the discrepancy, we have

$$\left| N_p(d_1, \ldots, d_k) - \frac{t}{g^k} \right| \leq Dt.$$

Hence, if D is much smaller than $1/g^k$ then all strings of length k appear approximately with the same frequency.

The following magnitude is important in the study of hyperelliptic curves. Let $T(p)$ be the largest t with the property that there exists a group $G \subset \mathbb{Z}_p^*$, $|G| = t$, such that for some $a_0 \in \mathbb{Z}_p^*$ all the smallest positive residues of $a_0 x$, $x \in G$, belong to the interval $[1, (p-1)/2]$. Clearly $T(p)$ is odd. Also, we claim that the following inequality holds

$$\max_{a \in \mathbb{Z}_p^*} |S(a, G)| > t/3.$$

Indeed, otherwise (1.7) holds with $\eta = 1/3$, and we can use Proposition 1.1 with $h = [p/4]$ and $n = (p+1)/2+h$. Hence, for some $x \in G$ we have

$$n + j \equiv a_0 x, x \in G, |j| \le h.$$

Therefore, $a_0 x$ is not congruent to any number from the interval $[1, (p-1)/2]$. Thus, we get the following.

Proposition 1.3. *Let t_0 be such that for every group $G \subset \mathbb{Z}_p^*$ of an odd order with $|G| > t_0$ we have*

$$\max_{a \in \mathbb{Z}_p^*} |S(a, G)| \le |G|/3.$$

Then $T(p) \le t_0$.

Estimates for exponential sums over subgroups are closely related to additive properties of subgroups.

Proposition 1.4. *Let $\delta > 0$ be such that*

$$|S(a, G)| \le |G|p^{-\delta} \quad (a \in \mathbb{Z}_p^*), \tag{1.5'}$$

$b_1, \dots, b_d \in \mathbb{Z}_p^*$. Then the number N of the solutions to the congruence

$$\sum_{j=1} b_j x_j \equiv 0 \quad (x_1, \dots, x_d \in X) \tag{1.12}$$

satisfies the inequality

$$\left| N - \frac{|G|^d}{p} \right| < |G|^d p^{-\delta d}. \tag{1.13}$$

In particular, $N > 0$ if $d \ge 1/\delta$.

We note that if δ and $d > 1/\delta$ are fixed and (1.5) holds for the family of pairs (p, G) then (1.13) gives an asymptotic formula for the number of the solutions of (1.12) as $p \to \infty$.

Proof of Proposition 1.4. We have

$$\begin{aligned} pN &= \sum_{x_1,\dots,x_d \in G} \sum_{a \in \mathbb{Z}_p} e\left(a \sum_{j=1} b_j x_j/p\right) \\ &= \sum_{a \in \mathbb{Z}_p} \prod_{j=1}^{d} \sum_{x_j \in G} e(a b_j x_j/p) \\ &= \sum_{a \in \mathbb{Z}_p} \prod_{j=1}^{d} S(a b_j, G). \end{aligned} \tag{1.14}$$

Separating the term $|G|^d$ corresponding to $a = 0$, we get

$$\begin{aligned} |pN - |G|^d| &= \left| \sum_{a \in \mathbb{Z}_p^*} \prod_{j=1}^{d} S(a b_j, G) \right| \\ &\le (p-1) \left(\max_{a \in \mathbb{Z}_p^*} |S(a, G)| \right)^d, \end{aligned}$$

and using (1.5') completes the proof of the proposition.

In a particular case $b_1 = \cdots = b_{d-1} = -1$, $b_d = b$, congruence (1.12) has a form

$$bx_d \equiv \sum_{j=1}^{d-1} x_j,$$

or

$$b \equiv \sum_{j=1}^{d-1} x_j/x_d.$$

Observing that $x_j/x_d \in G$ we obtain the following.

Corollary 1.5. *If (1.5') holds and $d \geq 1/\delta$ then for every $b \in \mathbb{Z}_p^*$ the congruence*

$$b \equiv \sum_{j=1}^{d-1} x_j, \quad x_j \in X$$

is solvable.

Corollary 1.5 gives a simple estimate for a number of summands in Waring problem for G.

To estimate $S(a, G)$ we need one more simple lemma.

Lemma 1.6. *For any $a \in \mathbb{Z}_p$ and $x \in G$ we have $S(a, G) = S(ax, G)$.*

Proof.

$$S(ax, G) = \sum_{y \in G} e(axy/p) = \sum_{z = xy, y \in G} e(az/p)$$
$$= \sum_{z \in G} e(az/p) = S(a, G).$$

Now we are ready to prove the simplest estimate for $|S(a, G)|$.

Theorem 1.7. *We have*

$$|S(a_0, G)| \le \sqrt{p} \quad (a_0 \in \mathbb{Z}_p^*). \tag{1.15}$$

Proof. By Lemma 1.6 and Lemma 1.2, we get

$$|G||S(a_0, G)|^2 = \sum_{x \in G} |S(a_0 x, G)|^2$$
$$\le \sum_{a \in G} |S(a, G)|^2 = p|G|,$$

and the theorem follows.

So, we have a nontrivial estimate for exponential sums over G (namely, (1.5')) provided that $|G| \geq p^{1/2+\delta}$. Our aim is to weaken this inequality for $|G|$.

However, it turns out that there is no nontrivial estimate

$$S(a, G) = o(|G|) \quad (p \to \infty, a \in \mathbb{Z}_p^*) \tag{1.4}$$

if $|G| \ll \log p$.

Theorem 1.8. *For every $u > 0$ there are $p(u)$ and $v > 0$ such that for $p \geq p(u)$ inequality*

$$|G| \leq u \log p \tag{1.16}$$

implies

$$\max_{a \in \mathbb{Z}_p^*} |S(a, G)| \geq v|G|.$$

Proof. Take some $T \in \mathbb{N}$, $T \leq t = |G|$, and some $X \subset G$ with $|X| = T$. By pigeonhole principle, there is an integer a, $1 \leq a < p$, such that $\|ax/p\| \leq p^{-1/T}$ for all $x \in X$, where $\|z\|$ denotes the distance form z to the nearest integer. Therefore, there is an interval $[\alpha, \beta) \in [0, 1)$, $\beta - \alpha \leq p^{-1/T}$, and a set $Y \subset X$, $|Y| \geq T/2$, such that $\{ax/p\} \in [\alpha, \beta)$ for all $x \in Y$. Thus, we have the following estimate for the discrepancy D of the set $\{ax/p : x \in G\}$:

$$D \geq \frac{|Y|}{t} - (\beta - \alpha) \geq \frac{|Y|}{t} - p^{1/T}. \tag{1.17}$$

If $|G| \leq \log p$ we take $T = t$. Then $|Y| \geq t/2$, and (1.17) implies

$$D \geq 1/2 - 1/e.$$

If $|G| > \log p$ (and, thus, $u > 1$) we take $T = [\log p/(3u)]$ and $p(u)$ so that $T \geq 1$ for $p \geq p(u)$. Then

$$|Y| \geq \max(1, [\log p/(6u)] > \log p/(12u),$$

and, by (1.17),

$$D > \frac{(\log p)/(12u)}{u \log p} - e^{-3u} = \frac{1}{12u^2} - e^{-3u} > 0.$$

So, in both cases we have $D \geq c(u) > 0$, and inequality

$$\max_{a \in \mathbb{Z}_p^*} |S(a, G)|/t \leq \eta \tag{1.7}$$

cannot hold for small $\eta > 0$ since it would imply

$$D \ll \eta(\log(\eta^{-1}) + 1).$$

But the last inequality is not compatible with our lower estimates for D if η is small enough. This completes the proof of Theorem 1.8.

Also, one can prove lower estimates for $|S(a,G)|$ using results on Turan's problem. Let t and N be positive integers. It is required to evaluate or to estimate

$$U_t(N) = \min_{\alpha_1,\dots,\alpha_t} \max_{a=1,\dots,N} \left| \sum_{j=1}^{t} e(a\alpha_j) \right|.$$

Taking $G = \{x_1, \dots, x_t\}$, $\alpha_j = e(x_j/p)$, we see that

$$\max_{a\in\mathbb{Z}_p^*} |S(a,G)| \geq U_t(p-1).$$

Theorem 1.8 follows from H. Montgomery's lower estimates for $U_t(p-1)$. H. Montgomery conjectured that for $a \in \mathbb{Z}_p^*$

$$|S(a,G)| \leq (1+\eta)\left(2t\log\frac{p^2}{t}\right)^{1/2},$$

where $\eta \to 0$ as $p \to \infty$. If this is true, then $S(a,G) = o(|G|)$ as $|G|/\log p \to \infty$.

Observe that neither of these proofs uses that G is a group. Thus, the following is true.

Theorem 1.8'. *For every $u > 0$ there are $p(u)$ and $v > 0$ such that for $p \geq p(u)$ and $X \subset \mathbb{Z}_p$ inequality*

$$|X| \leq u \log p \tag{1.16'}$$

implies

$$\max_{a \in \mathbb{Z}_p^*} \left| \sum_{x \in X} e(ax/p) \right| \geq v|X|.$$

To get better estimates for $S(a, G)$ we define, for $k \in \mathbb{N}$, $T_k(G)$ as the number of the solutions to the congruence

$$x_1 + \cdots + x_k \equiv x_{k+1} + \cdots + x_{2k}, \quad x_j \in G.$$

Clearly, $T_1(G) = t$, and, for any k,

$$t^k \leq T_k(G) \leq t^{2k-1}. \tag{1.17}$$

Identity (1.14) in our case can be written as

$$pT_k(G) = \sum_{a \in \mathbb{Z}_p} |S(a, G)|^{2k}. \tag{1.18}$$

It easily follows from (1.18) that

$$T_k(G) \geq |S(0,G)|^{2k}/p = t^{2k}/p \tag{1.19}$$

and

$$T_{k+1}(G)/t^{2(k+1)} \leq T_k(G)/t^{2k}. \tag{1.20}$$

Moreover, (1.18) shows that $T_k(G)/t^{2k}$ is close to $1/p$ for large k if all sums $|S(a,G)|$, $a \in \mathbb{Z}_p^*$, are small. In particular, it follows from Proposition 1.4 or directly from (1.18) that if we have

$$S(a,G) \leq |G|p^{-\delta} \quad (a \in \mathbb{Z}_p^*), \tag{1.5'}$$

and $2k \geq 1/\delta$, then $T_k(G) \leq 2t^{2k}/p$. We will show now that, conversely, if $T_k(G)$ is close to t^{2k}/p for some small k, then we can get bound $|S(a,G)|$ well.

Proposition 1.9. *We have*

$$|S(a_0,G)| \leq (pT_k(G)/t)^{1/(2k)} \quad (a_0 \in \mathbb{Z}_p^*). \tag{1.21}$$

Proof. By Lemma 1.6 and (1.18), we get

$$t|S(a_0,G)|^{2k} = \sum_{x\in G} |S(a_0x,G)|^2$$
$$\le \sum_{a\in G} |S(a,G)|^{2k} = pT_k(G),$$

and the proposition follows.

In particular, if $T_k(G)/t^{2k} \le tp^{-\varepsilon}/p$ then

$$|S(a,G)| \le |G|p^{-\varepsilon/(2k)} \quad (a\in\mathbb{Z}_p^*).$$

Observe that Theorem 1.7 is a particular case of Proposition 1.9 for $k = 1$. If we use a trivial estimate $T_k(G) \le t^{2k-1}$ we get only

$$|S(a,G)| \le \left(pt^{2k-1}/t\right)^{1/(2k)} = t(p/t^2)^{1/(2k)}.$$

This estimate is worse than the trivial one $|S(a,G)| \le t$ if $|G| < p^{1/2}$ and worse than the simplest estimate $|S(a,G)| \le p^{1/2}$ if $|G| > p^{1/2}$. However, if $|G|$ is close to $p^{1/2}$ then any improvement of the trivial inequality $T_k(G) \le t^{2k-1}$ will improve estimates for $|S(a,G)|$.

Lecture 2

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 $\mathbb{Z}_p$. We take an arbitrary subgroup G of the group $\mathbb{Z}_p^*$. Let $t = |G|$. For brevity, we will write $a \equiv b$ instead of $a \equiv b (\mathrm{mod} p)$.

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 $a \in \mathbb{Z}_p$.

The main subject of my talks is the estimation of exponential sums over G:

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

We can estimate $S(a, G)$ trivially:

$$|S(a,G)| \le \sum_{x\in G} |e(ax/p)| = \sum_{x\in G} 1 = |G|. \tag{1.3}$$

Clearly, inequality (1.3) is equality if $a = 0$. We are interested in obtaining nontrivial estimates for $S(a, G)$:

$$S(a,G) = o(|G|) \quad (p \to \infty, a \in \mathbb{Z}_p^*) \tag{1.4}$$

or, for some $\delta > 0$.

$$S(a,G) \ll |G|p^{-\delta} \quad (a \in \mathbb{Z}_p^*). \tag{1.5}$$

We proved the simplest estimate for $|S(a, G)|$.

Theorem 1.7. *We have*

$$|S(a,G)| \le \sqrt{p} \quad (a \in \mathbb{Z}_p^*). \tag{1.15}$$

So, we have a nontrivial estimate for exponential sums over G (namely, (1.5)) provided that $|G| \ge p^{1/2+\delta}$. Our aim is to weaken this inequality for $|G|$.

To get better estimates for $S(a,G)$ we define, for $k \in \mathbb{N}$, $T_k(G)$ as the number of the solutions to the congruence

$$x_1 + \cdots + x_k \equiv x_{k+1} + \cdots + x_{2k}, \quad x_j \in G.$$

Clearly, $T_1(G) = t$, and, for any k,

$$t^k \le T_k(G) \le t^{2k-1}. \tag{1.17}$$

Also, we have

$$pT_k(G) = \sum_{a \in \mathbb{Z}_p} |S(a,G)|^{2k}. \tag{1.18}$$

It easily follows from (1.18) that

$$T_k(G) \ge |S(0,G)|^{2k}/p = t^{2k}/p. \tag{1.19}$$

We proved the following.

Proposition 1.9. *We have*

$$|S(a,G)| \le (pT_k(G)/t)^{1/(2k)} \quad (a \in \mathbb{Z}_p^*). \tag{1.21}$$

In particular, if $T_k(G)/t^{2k} \le tp^{-\varepsilon}/p$ then

$$|S(a,G)| \le |G| p^{-\varepsilon/(2k)} \quad (a \in \mathbb{Z}_p^*).$$

Observe that Theorem 1.7 is a particular case of Proposition 1.9 for $k = 1$. If we use a trivial estimate $T_k(G) \le t^{2k-1}$ we get only

$$|S(a,G)| \le \left(pt^{2k-1}/t\right)^{1/(2k)} = t(p/t^2)^{1/(2k)}.$$

This estimate is worse than the trivial one $|S(a,G)| \le t$ if $|G| < p^{1/2}$ and worse than the simplest estimate $|S(a,G)| \le p^{1/2}$ if $|G| > p^{1/2}$. However, if $|G|$ is close to $p^{1/2}$ then any improvement of the trivial inequality $T_k(G) \le t^{2k-1}$ will improve estimates for $|S(a,G)|$.

Such an improvement was made by Shparlinski who used the following result of A. Garcia and J. F. Voloch.

Theorem 2.1. *For $b \in \mathbb{Z}_p$ denote by $N_2(b)$ the number of solutions to the congruence $x_1 + x_2 \equiv b$, $x_1, x_2 \in G$. If*

$$|G| < \frac{p-1}{(p-1)^{1/4}+1}, \tag{2.1}$$

then for any $b \in \mathbb{Z}_p^*$ we have

$$N_2(b) \le 4|G|^{2/3}. \tag{2.2}$$

Using (2.2), one can nontrivially estimate $T_2(G)$ provided that (2.1) holds. Recall that $T_2(G)$ is the number of solutions to

$$x_1 + x_2 \equiv x_3 + x_4, \quad x_j \in G. \tag{2.3}$$

The number of solutions to (2.3) with $x_3 + x_4 \equiv 0$ is at most $|G|^2$. Next, if $x_3 + x_4 \not\equiv 0$, then, by (2.2), there are at most $4|G|^{2/3}$ pairs (x_1, x_2) satisfying (2.3) Therefore,

$$T_2(G) \leq p^2 + 4p^{8/3} < 5p^{8/3}. \tag{2.4}$$

Now we can estimate exponential sums using Proposition 1.9

$$|S(a, G)| \leq (pT_k(G)/t)^{1/(2k)} \quad (a \in \mathbb{Z}_p^*). \tag{1.21}$$

for $k = 2$:

$$|S(a, G)| \leq (5p)^{1/4}|G|^{5/12} \quad (a \in \mathbb{Z}_p^*).$$

This is better than the estimate $p^{1/2}$ for $|G| \leq p^{3/5-\delta}$, $p \geq p(\delta)$, and better than the trivial $|G|$ for $|G| \geq p^{3/7+\delta}$, $p \geq p(\delta)$. Observing that (2.1) holds for $|G| \leq p^{3/4-\delta}$, $p \geq p(\delta)$. Thus, the improvement was made for $p^{3/7+\delta} \leq |G| \leq p^{3/5-\delta}$, $p \geq p(\delta)$.

D. R. Heath-Brown succeeded in applying Stepanov's method to the proof of the theorem of Garcia and Voloch. Moreover, in our joint paper we used his technique to improve estimate (2.4) for $T_2(G)$ if $|G| \le p^{2/3}$.

Theorem 2.2. *If* $|G| \le p^{2/3}$, *then*

$$T_2(G) \ll |G|^{5/2}. \tag{2.5}$$

We are not able to improve the estimate of Garcia and Voloch

$$N_2(b) \ll |G|^{2/3}$$

for all $b \in \mathbb{Z}_p^*$, but it can be improved in average, and this implies (2.5). I shall present the proof of (2.5), but first let us discuss its applications. To estimate exponential sums $S(a, G)$, one can use Proposition 1.9; however, the following more general fact sometimes gives better estimates.

Theorem 2.3. *If $k, l \in \mathbb{N}$, $a \in \mathbb{Z}_p^*$, then*

$$|S(a,G)| \le \left(pT_k(G)T_l(G)\right)^{1/(2kl)} t^{1-1/k-1/l}. \tag{2.6}$$

Clearly, for $l = 1$ Theorem 2.3 is just Proposition 1.9. For $k = l$ (2.6) can be written as

$$|S(a,G)| \le \left(\frac{T_k(G)p^{1/2}}{t^{2k}}\right)^{1/(k^2)} t. \tag{2.7}$$

Clearly, (2.7) supersedes the trivial estimate $|S(a,G)| \le t$ if and only if

$$T_k(G) < t^{2k}p^{-1/2}. \tag{2.8}$$

In the most interesting case $|G| < p^{1/2}$ (2.8) is weaker than the condition $T_k(G) < t^{2k}t/p$ required to have any benefit from Proposition 1.9.

Theorem 2.3 probably has to be attributed to A. A. Karatsuba who in fact proved the following.

Theorem 2.4. *Let $X \subset \mathbb{Z}_p^*$. For $k \in \mathbb{N}$ by $T_k(X)$ denote the number of the solutions to the congruence*

$$x_1 + \cdots + x_k \equiv x_{k+1} + \cdots + x_{2k}, \quad x_j \in X.$$

Then for $k, l \in \mathbb{N}$, $a \in \mathbb{Z}_p^*$, we have

$$\left| \sum_{x,y \in X} e(axy/p) \right| \le (pT_k(X)T_l(X))^{1/(2kl)} |X|^{2-1/k-1/l}.$$

Theorem 2.4 is similar to the results proven for estimates of H. Weil's sums by I. M. Vinogradov's method. Theorem 2.3 is contained in Theorem 2.4 since

$$\sum_{x,y \in G} e(axy/p) = |G| \sum_{z \in G} e(az/p) = |G| S(a, G).$$

Combining Theorem 2.2 with Theorem 2.3 for $k = 1, l = 2$ if $p^{1/2} < |G| \le p^{2/3}$ and for $k = l = 2$ if $|G| \le p^{1/2}$ we get for $a \in \mathbb{Z}_p^*$

$$|S(a, G)| \ll p^{1/4} |G|^{3/8} \quad (p^{1/2} < |G| \le p^{2/3}), \tag{2.9}$$

$$|S(a, G)| \ll p^{1/8} |G|^{5/8} \quad (|G| \le p^{1/2}). \tag{2.10}$$

Observe that (2.9) supersedes the simplest estimate $|S(a,G)| \le p^{1/2}$ for $|G| \le p^{2/3-\delta}$, $p \ge p(\delta)$, and (2.10) supersedes the trivial estimate $|S(a,G)| \le |G|$ for $|G| \ge p^{1/3+\delta}$, $p \ge p(\delta)$. For $|G| \ge p^{2/3}$ we cannot prove anything better than $|S(a,G)| \ll p^{1/2}$.

Let me recall the definition of $1/p$-pseudo-random generators of Blum, Blum, and Shub. Take an integer $g \ge 2$. We consider the g-ary expansion of $1/p$. If g is fixed then we can expect (and this is true indeed) that for many primes p there is no large correlation among close digits in this expansion, and we can talk about a pseudo-random generator. Let G be the subgroup of $\mathbb{Z}_p^*$ generated by g, $t = |G|$. It is easy to see that t is the (least) period of the g-ary expansion of $1/p$. We are interested in appearances of a sequence $(d_1, \dots, d_k)$ of g-ary digits in the expansion. We have proved that if

$$\max_{a \in \mathbb{Z}_p^*} |S(a,G)|/t \le \eta \tag{1.7}$$

and

$$\frac{p}{2g^k} - 1 \ge \eta p/(1+\eta) \tag{2.11}$$

then the g-ary expansion of $1/p$ contains any string of length k. It is easy to see that (2.11) holds if $k \le (\log(1/\eta) - C)/\log g$ for some absolute constant C.

Let me stress that we do not expect that the digits of the g-ary expansion of $1/p$ are well-distributed for ALL large p. For example, take $g = 2$. If p is a Mersenne prime (that is, $p = 2^q - 1$), then the expansion has the string $(0, \dots, 0, 1)$ of size q as its period; thus, the sequence is very far from being pseudo-random. However, we can say that for ALMOST ALL primes the sequence of digits is in a sense well-distributed.

Fix g and take a large $L \in \mathbb{N}$. Also,let $T \in \mathbb{N}$. Let us estimate the number N of primes $p \le g^L$ such that the order of g in $\mathbb{Z}_p$ is at most T. We have

$$N \le \sum_{t \le T} |\{p : \, g^t \equiv 1 (\mathrm{mod} p)\}| = \sum_{t \le T} w(g^t - 1)$$
$$\ll \sum_{t \le T} t \le T^2.$$

On the other hand, the number of primes $p \le g^L$ is $\gg g^L/L$. Therefore, for every fixed $\varepsilon > 0$, specifying $T = g^{(1/2-\varepsilon)L}$, we see that for almost all primes $p \le g^L$ the order of g in $\mathbb{Z}_p$ is $> T \ge p^{1/2-\varepsilon}$. This means that the proportion of exceptional primes amongst all the primes $\le g^L$ tends to 0 as $L \to \infty$.

Next, if G is the subgroup of $\mathbb{Z}_p^*$ generated by g, $t = |G| > p^{1/2-\varepsilon}$, than, by (2.9) and (2.10),

$$|S(a,G)| \ll p^{1/4}|G|^{3/8} \quad (p^{1/2} < |G| \le p^{2/3}), \tag{2.9}$$

$$|S(a,G)| \ll p^{1/8}|G|^{5/8} \quad (|G| \le p^{1/2}). \tag{2.10}$$

we have

$$\max_{a\in\mathbb{Z}_p^*} |S(a,G)|/t \le \eta$$

with $\eta \ll p^{-\frac{1}{16}+\frac{3}{8}\varepsilon}$. This implies, that the g-ary expansion of $1/p$ contains any string of length
$\le (\frac{1}{16}-\frac{3}{8}\varepsilon)L - C$. Moreover, for large L all the strings of length $\le (\frac{1}{16}-\varepsilon)L$ will appear with approximately the same frequency. Observe that we cannot prove any results of this type using the simplest estimate $|S(a,G)| \le p^{1/2}$.

We (SK, I. Shparlinski) can prove more: for almost all primes $p \le g^L$ the g-ary expansion of $1/p$ contains any string of length $\le \frac{3}{37}L$.

Now we shall make some preparations to prove the estimate for $T_2(G)$. Take some cosets $G_1, \dots, G_s$ of the group G in $\mathbb{Z}_p^*$. For any coset G_j denote

$$N_j = |\{x \in G : \, x - 1 \in G_j\}|.$$

Lemma 2.5. *Let $|G| = t$ and suppose that a positive integer L satisfies the conditions*

$$L < t, \quad tL \le p, \quad s < L^3/(2t). \tag{2.12}$$

Then

$$\sum_{j=1}^{s} N_j \le \frac{2tL}{[t/L]}.$$

Proof. Let $K = [t/L]$. We shall begin by taking a polynomial $\Phi(X, Y, Z)$, for which

$$\deg_X \Phi < K, \quad \deg_Y \Phi < L, \quad \deg_Z \Phi < L.$$

For $j = 1, \dots, s$ we define the sets

$$R_j = \{x \in G : \, x - 1 \in G_j\}, \quad R = \bigcup_{j=1}^{s} R_j.$$

Clearly,

$$\sum_{j=1}^{s} N_j = |R|.$$

The underlying idea is then to arrange that the polynomial

$$\Psi(X) = \Phi(X, X^t, (X-1)^t)$$

has a zero of order at least K at each point $x \in R$. We will therefore be able to conclude that

$$K \sum_{j=1}^{s} N_j \leq \deg \Psi,$$

provided that Ψ does not vanish identically. We note that

$$\deg \Psi \leq \deg_X \Phi + t \deg_Y \Phi + t \deg_Z \Phi \leq K - 1 + 2t(L-1),$$

whence

$$\sum_{j=1}^{s} N_j \leq \frac{K - 1 + 2t(L-1)}{K} < \frac{2tL}{[t/L]},$$

provided that Ψ does not vanish identically.

In order for Ψ to have a zero of multiplicity at least K at a point x, we need

$$\left(\frac{d}{dx}\right)^n \Psi(X)\Big|_{X=x} = 0 \quad (n < K).$$

Since $x \neq 0, 1$ for $x \in R$, this will be equivalent to

$$(X(X-1))^n \left(\frac{d}{dx}\right)^n \Psi(X)\Big|_{X=x} = 0. \tag{2.13}$$

We now observe that

$$X^m \left(\frac{d}{dx}\right)^m X^u = \frac{u!}{(u-m)!} X^u,$$

$$X^m \left(\frac{d}{dx}\right)^m X^{tv} = \frac{(tv)!}{(tv-m)!} X^{tv},$$

$$(X-1)^m \left(\frac{d}{dx}\right)^m (X-1)^{tw} = \frac{(tw)!}{(tw-m)!} (X-1)^{tw}.$$

It follows that

$$(X(X-1))^k \left(\frac{d}{dX}\right)^k X^u X^{tv} (X-1)^{tw}$$
$$= P_{k,u,v,w}(X) X^{tv} (X-1)^{tw}$$

where $P_{k,u,v,w}$ either vanishes or is a polynomial of degree at most $k+u$. We therefore deduce that for any $j = 1, \ldots, s$ and for any $x \in R_j$, we have

$$(X(X-1))^k \left(\frac{d}{dx}\right)^k X^u X^{tv} (X-1)^{tw} \Big|_{X=x}$$
$$= a_j^w P_{k,u,v,w}(x)$$

where $a_j = y^t$ for $y \in G_j$; the crucial argument here is that y^t does not depend on the choice of $y \in G$ or $y \in G_j$.

We now write

$$\Phi(X, Y, Z) = \sum_{u,v,w} \lambda_{u,v,w} X^u Y^v Z^w$$

and

$$P_{k,j}(X) = \sum_{u,v,w} \lambda_{u,v,w} a_j^w P_{k,u,v,w}(X)$$

so that $\deg P_{k,j} < A + k$ and

$$(X(X-1))^k \left(\frac{d}{dX}\right)^k \Phi(X, X^t, (X-1)^t)\Big|_{X=x} = P_{k,j}(x)$$

for any $x \in R_j$. We shall arrange, by appropriate choice of the coefficients $\lambda_{u,v,w}$, that $P_{k,j}(X)$ vanishes identically for $k < K$. This will ensure that

$$(X(X-1))^n \left(\frac{d}{dx}\right)^n \Psi(X)\Big|_{X=x} = 0 \tag{2.13}$$

holds at every point $x \in R$. Each polynomial $P_{k,j}(X)$ has at most $K + k < 2K$ coefficients which are linear forms in the original $\lambda_{u,v,w}$. Thus if

$$sK(2K) < KL^2, \tag{2.14}$$

there will be a set of coefficients $\lambda_{u,v,w}$, not all zero, for which the polynomials $P_{k,j}(X)$ vanish for all $k < K$. But, since $K = [t/L] \le t/L$ and $s < L^3/(2t)$,

$$sK(2K) = 2sK^2 \le 2sKt/L < KL^2,$$

and (2.14) holds.

We must now consider whether the polynomial $\Phi(X, X^t, (X-1)^t)$ can vanish if $\Phi(X, Y, Z)$ does not. We shall write

$$\Phi(X, Y, Z) = \sum_w \Phi_w(X, Y) Z^w,$$

and take w_0 to be the smallest value w for which $\Phi_w(X, Y)$ is not identically zero. It follows that

$$\begin{aligned} &\Phi(X, X^t, (X-1)^t) \\ &= (X-1)^{tw_0} \sum_{w_0 \le w \le B} \Phi_w(X, X^t)(X-1)^{t(w-w_0)}, \end{aligned}$$

so that if $\Phi(X, X^t, (X-1)^t)$ is identically zero, we must have

$$\Phi_{w_0}(X, X^t) \equiv 0 (\mathrm{mod} (X-1)^t). \tag{2.15}$$

We show, by induction on N, that if a polynomial $f(X) \in \mathbb{Z}_p[X]$ of degree $\deg f < p$ is a sum of $N \geq 1$ distinct monomials, then $(X-1)^N$ cannot divide $f(X)$. The case $N = 1$ is trivial. Now suppose that $N > 1$ and let

$$f(X) = \sum_w c_w x^W$$

where w runs over N distinct values. Then the polynomial

$$g(X) = Xf'(X) - Wf(X) = \sum_w c_w(w - W)X^w,$$

where $W = \deg w$, contains exactly $N - 1$ terms. (Notice that $c_w(w - W) \in \mathbb{Z}_p$ is nonzero for $w < W$ since $W < p$.) We then see that if $(X-1)^N$ divides $f(X)$, then $(X-1)^{N-1}$ divides $g(X)$ contrary to our induction hypothesis.

We have

$$\deg \Phi_{w_0}(X, X^t) \leq K - 1 + t(L-1) < tL.$$

Therefore, the congruence

$$\Phi_{w_0}(X, X^t) \equiv 0 (\mathrm{mod} (X-1)^t) \tag{2.15}$$

is impossible provided that $KL \leq t$, $tL \leq p$. But these inequalities hold, and Lemma 2.5 is proven.

Now take all the cosets $G_1, \dots, G_n$ of the group G in $\mathbb{Z}_p^*$; thus, $n = (p-1)/t$. Again, for any coset G_j we denote

$$N_j = |\{x \in G : \, x - 1 \in G_j\}|.$$

Hence,

$$N_j = |\{x \in G, y \in G_j : \, x - 1 \equiv y\}|,$$

$$tN_j = |\{x_1, x_2 \in G, y \in G_j : \, x_1 - x_2 \equiv y\}|,$$

and for any $y \in G_j$ we have

$$N_j = |\{(x_1, x_2) \in G : \, x_1 - x_2 \equiv y\}|.$$

Therefore,

$$\begin{aligned} T_2(G) &= |\{(x_1, x_2, x_3, x_4) : \, x_j \in G, x_1 - x_2 \equiv x_3 - x_4\}| \\ &= \sum_{y \in \mathbb{Z}_p} |\{(x_1, x_2) : \, x_1, x_2 \in G, x_1 - x_2 \equiv y\}|^2 \\ &\le t^2 + \sum_{j=1}^{n} \sum_{y \in G_j} |\{(x_1, x_2) : \, x_1, x_2 \in G, x_1 - x_2 \equiv y\}|^2 \\ &= t^2 + \sum_{j=1}^{n} \sum_{y \in G_j} N_j^2 = t^2 + t \sum_{j=1}^{n} N_j^2. \end{aligned} \tag{2.16}$$

Also, observe that

$$t^2 = \sum_{y\in\mathbb{Z}_p} |\{(x_1,x_2):\, x_1,x_2\in G, x_1-x_2\equiv y\}|$$
$$\geq \sum_{j=1}^{n}\sum_{y\in G_j} |\{(x_1,x_2):\, x_1,x_2\in G, x_1-x_2\equiv y\}|$$
$$= \sum_{j=1}^{n}\sum_{y\in G_j} N_j = t\sum_{j=1}^{n} N_j.$$

Hence,

$$\sum_{j=1}^{n} N_j \leq t. \tag{2.17}$$

Now we are in position to prove Theorem 2.2.

Theorem 2.2. *If $|G|\leq p^{2/3}$, then*

$$T_2(G) \ll |G|^{5/2}. \tag{2.5}$$

We assume that $t=|G|$ is large enough and the cosets $G_1,\dots,G_n$ are ordered in such a way that

$$N_1 \geq N_2 \cdots \geq N_n.$$

Then for $1 \le s \le t^{1/2}/3$ and $L = [(2st)^{1/3}] + 1$ the conditions

$$L < t, \quad tL \le p, \quad s < L^3/(2t). \tag{2.12}$$

of Lemma 2.5 are satisfied, and it can be applied giving

$$\sum_{j=1}^{s} N_j \ll s^{2/3} t^{2/3}.$$

Hence,

$$N_s \ll s^{-1/3} t^{2/3} \quad (s \le t^{1/2}/3). \tag{2.18}$$

For $s > t^{1/2}/3$ the following estimate holds:

$$N_s \le N_{[t^{1/2}/3]} \ll t^{1/2}. \tag{2.19}$$

Using (2.16) and combining the bounds (2.18) and (2.19) with (2.17) we get

$$T_2(G) \leq t^2 + t\sum_{s=1}^{n} N_s^2$$

$$\leq t^2 + t \sum_{s \leq t^{1/2}/3} N_s^2 + t \sum_{s > t^{1/2}/3} N_s^2$$

$$\ll t^2 + t \sum_{s \leq t^{1/2}/3} \left(s^{-1/3}t^{2/3}\right)^2 + t \sum_{s > t^{1/2}/3} t^{1/2} N_s$$

$$\ll t^2 + t \sum_{s \leq t^{1/2}/3} \left(s^{-1/3}t^{2/3}\right)^2 + t(t^{1/2})t \ll t^{5/2},$$

and we have the desired result.

Now we will prove a corollary from Lemma 2.5. If $*$ is a binary operation on $\mathbb{Z}_p$, $A, B \subset \mathbb{Z}_p$, then we denote

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

Corollary 2.7. *(A. Glibichuk.) Let $B \subset G$ and $0 < |B| \le p^{1/2}$. Then*

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

Proof. Let $G_1, \ldots, G_s$ be all the cosets of G in $\mathbb{Z}_p^*$ containing elements from $B-B$. Then $G_j \subset G(B-B)$ for $j = 1, \ldots, s$, and hence

$$|G(B-B)| = s|G| + 1. \tag{2.21}$$

Inequality (2.20) follows immediately from (2.21) for $s > |B|^{3/2}/(17|G|)$ (and, in particular, for $|G| > |B|^{3/2}/17$). Thus, we can assume that

$$|G| \le |B|^{3/2}/17, \quad s \le |B|^{3/2}/(17|G|). \tag{2.22}$$

Also, assume that $|B|$ is large enough. Fixed $x_0 \in B$. Recall that

$$N_j = |\{x \in G : \, x - 1 \in G_j\}|.$$

Equivalently,

$$N_j = |\{x \in G : \, x - x_0 \in G_j\}|.$$

Since for every $x \in B \setminus \{x_0\}$ we have $x - x_0 \in G_j$ for some $j = 1, \ldots, s$,

$$|B| - 1 = \sum_{j=1}^{s} |\{x \in B : x - x_0 \in G_j\}| \le \sum_{j=1}^{s} N_j. \tag{2.23}$$

Take $L = [(2st)^{1/3}] + 1$. Now we can use Lemma 2.5.

Lemma 2.5. *Let $|G| = t$ and suppose that a positive integer L satisfies the conditions*

$$L < t, \quad tL \le p, \quad s < L^3/(2t). \tag{2.12}$$

Then

$$\sum_{j=1}^{s} N_j \le \frac{2tL}{[t/L]}.$$

We have

$$L \le [(2|B|^{3/2}/17)^{1/3}] + 1 < (|B| - 1)^{1/2}/2. \tag{2.24}$$

Therefore,

$$L < |B|^{1/2} \le |B| \le t,$$

$$tL < (|B|^{3/2}/17)(|B|^{1/2}) < |B|^2 < p.$$

So, (2.12) are fulfilled. By Lemma 2.5 and (2.24),

$$\sum_{j=1}^{s} N_j \le 4L^2 < |B| - 1,$$

but his does not agree with (2.23), and Corollary 2.7 follows.

Using Stepanov— Heath-Brown's method, Theorem 2.2 can be extended to $k > 2$ provided that $|G| \le p^{1/2}$.

Theorem 2.8. *If* $|G| \le p^{1/2}$, $k \in \mathbb{N}$, *then*

$$T_k(G) \ll_k |G|^{2k-2+2^{1-k}}. \tag{2.25}$$

It follows from Theorem 2.3 that we can get nontrivial estimates for exponential sums if for some k and $\varepsilon > 0$ we have

$$T_k(G) \ll_{k,\varepsilon} |G|^{2k} p^{-1/2-\varepsilon}. \tag{2.26}$$

Namely, (2.26) implies $|S(a, G)| \ll_{k,\varepsilon} p^{-\varepsilon/k^2}|G|$ for $a \in \mathbb{Z}_p^*$. By Theorem 2.8, (2.26) holds for

$$|G| \ge p^{1/4+\varepsilon} \tag{2.27}$$

and $k \ge k(\varepsilon)$. Thus, we have nontrivial estimates for exponential sums under supposition (2.27).

It is likely that Theorem 2.8 and restriction (2.27) correspond to natural thresholds of Stepanov— Heath-Brown's method.

Let me mention a corollary from Theorem 2.8. For $b \in \mathbb{Z}_p$, $k \in \mathbb{N}$ we denote by $N_k(b)$ the number of the solutions to the congruence

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

It is not difficult to prove that

$$\sum_{b \in kG} N_k(b) = |G|^k,$$

$$\sum_{b \in kG} N_k(b)^2 = T_k(G)$$

(we have checked this for $k = 2$). Hence, by Cauchy— Schwartz inequality

$$|kG| \geq |G|^{2k}/T_k(G),$$

and from Theorem 2.8 we get the following.

Corollary 2.9. *If* $|G| \leq p^{1/2}$, $k \in \mathbb{N}$, *then*

$$|kG| \gg_k |G|^{2-2^{1-k}}. \tag{2.28}$$

To weaken restriction

$$|G| \geq p^{1/4+\varepsilon} \tag{2.27}$$

we had to show that for $|G| \leq p^{1/4}$ and for some k and ε

$$T_k(G) \ll |G|^{2k-2-\varepsilon}.$$

This would imply

$$|kG| \gg |G|^{2+\varepsilon}.$$

But before 2003 it was not clear how to exclude the situation

$$\forall k \, \exists p, G : \, |G| \leq p^{1/4}, |kG| < |G|^2. \tag{2.29}$$

Now it is time to have an excursion to a very exciting number theoretical and combinatorial problem.

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, $|A| \le p^{1/2}$. This would exclude

$$\forall k \, \exists p, G : \, |G| \le p^{1/4}, N_k(G) < |G|^2. \tag{2.29}$$

Indeed, take a large k and use (2.29) with k replaced by k^2. Then we have $|G| \le p^{1/4}$,

$$|kG| \gg_k |G|^{2-2^{1-k}}, \tag{2.28}$$

but, by (2.29),

$$|k^2G| < |G|^2. \tag{2.31}$$

This inequality implies

$$|kG| \le |k^2G| < p^{1/2}.$$

Since

$$kG + kG = 2kG, \quad (kG)(kG) \subset k^2G,$$

we deduce from conjectural (2.30)

$$|k^2G| \ge \max(kG + kG, (kG)(kG)) \gg_k |G|^{\left(2-2^{1-k}\right)(1+\alpha)},$$

but this does not agree with (2.30) for $k = k(\alpha)$ and sufficiently large p.

Unfortunately no existing proofs of (2.30) for integer, real or complex numbers could be used for $\mathbb{Z}_p$.

Lecture 3

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* $0 < |A| \le \sqrt{p}$ *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, $|I(A)| \ge |A - A|$, 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

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

then

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

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

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,

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

Therefore,

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

(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

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

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 $|S_\xi(A)| \le p < |A|^2$ 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*

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

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,

$$|I(A)| \geq |S_\xi(A)| \geq \min\left(|A|u, |A|^2|H|/(|A|^2+|H|)\right)$$

$$\geq \min(2|A|^3/(9|AA|), |A|^2/2, |H|/2). \tag{3.12}$$

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 $k \leq k(\delta)$ and $C = C(\delta)$:

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

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

$$\left|\sum_{x\in G} e(ax/p)\right|^k$$

$$= \left(\sum_{x\in G} e(ax/p)\right)^{k/2} \left(\sum_{x\in G} e(-ax/p)\right)^{k/2}$$

$$= \sum_{x_1,\dots,x_k\in G} e\left(a(x_1 - x_2 + \cdots + x_{k-1} - x_k)/p\right)$$

$$= \sum_y B_k(G,y)e(ay/p).$$

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 $Y' = Y_1$, $A' = A_1$

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

$$\left|\sum_{y\in Y'} B_k(G,y)e(ay/p)\right| \geq U := \omega|G|^k \quad (a \in A'), \tag{3.23}$$

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

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

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

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

$$|A_3| \ge \omega|A_1|,$$

$$\left|\sum_{x\in X_1}\sum_{y\in Y_2} B_k(G,x)B_k(G,y)e(axy/p)\right|$$

$$\ge \omega U'|H|^{2k} \quad (a \in A_3), \tag{3.26}$$

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

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

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

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

$$y_1 y_2 \equiv y_3 y_4, \quad y_j \in Y_2. \tag{3.27}$$

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

$$|Y_4 Y_4| \leq |Y_3 Y_3|,$$

we conclude that both the sets $Y_4 + Y_4$, $Y_4 Y_4$ 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*

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