On exponential sums and equations over multiplicative subgroups in finite field.

Iurii Shteinikov, joint work with B. Murphy, M. Rudnev and I. Shkredov

Steklov Mathematical Institute

Marseille, UDT 2018

Beginning

1. p large prime number.
2. $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$ - residue ring modulo q, $\mathbb{Z}_q^*$ – the set of invertible elements of $\mathbb{Z}_q$,
3. $e_q(x) := e^{2\pi i x/q}$.

Some definitions

1. Let $G \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ be some multiplicative subgroup of the field $\mathbb{Z}/p\mathbb{Z}$.
2. Exponential sums over subgroup G are the following quantities $S(a, G)$

$$S(a, G) = \sum_{g \in G} \exp\{2\pi i \frac{ag}{p}\}.$$

3. Gauss sums $S_n(a, p)$ are defined as follows

$$S_n(a, p) = \sum_{0 \le x \le p-1} \exp\{2\pi i \frac{ax^n}{p}\}.$$

4. I am planning to speak about upper bounds for $|S(a, G)|$, and connected with them other quantities. The firs question is to obtain some kind of nontrivial estimates of the type $|S(a, G)| = o(|G|)$.

Some history

If G– the subgroup of quadratic residues, these sums are calculated explicitly

$$S_{2,p}(a) = i^{(\frac{p-1}{2})^2} \left(\frac{a}{p}\right) \sqrt{p}.$$

In general case we always have

$$|S(a, G)| < \sqrt{p}.$$

So there is a question how to estimate $|S(a, G)|$ where $|G| \leq \sqrt{p}$.

Some history

If G– the subgroup of quadratic residues, these sums are calculated explicitly

$$S_{2,p}(a) = i^{(\frac{p-1}{2})^2} \left(\frac{a}{p}\right) \sqrt{p}.$$

In general case we always have

$$|S(a, G)| < \sqrt{p}.$$

So there is a question how to estimate $|S(a, G)|$ where $|G| \leq \sqrt{p}$.

Some history

If G– the subgroup of quadratic residues, these sums are calculated explicitly

$$S_{2,p}(a) = i^{(\frac{p-1}{2})^2} \left(\frac{a}{p}\right) \sqrt{p}.$$

In general case we always have

$$|S(a, G)| < \sqrt{p}.$$

So there is a question how to estimate $|S(a, G)|$ where $|G| \leq \sqrt{p}$.

Related tasks and fields

Pseudo-random sequences;

Special equations, distribution of elements of subgroups in finite field

For integer $m \geq 1$ let $T_m(G)$ denotes the number of solutions of the following equation

$$x_1 + \ldots + x_m = y_1 + \ldots + y_m \pmod p, x_i, y_j \in G.$$

Estimates for $|S(a,G)|$ can be obtained using the following Theorem.

Theorem

For any integers $m, l \geq 1$ we have the following inequality :

$$|S(a,G)| \leq (pT_l(G)T_m(G))^{\frac{1}{2lm}} |G|^{1-\frac{1}{l}-\frac{1}{m}}.$$

For integer $m \geq 1$ let $T_m(G)$ denotes the number of solutions of the following equation

$$x_1 + \ldots + x_m = y_1 + \ldots + y_m \pmod p, x_i, y_j \in G.$$

Estimates for $|S(a, G)|$ can be obtained using the following Theorem.

Theorem

For any integers $m, l \geq 1$ we have the following inequality :

$$|S(a, G)| \leq (pT_l(G)T_m(G))^{\frac{1}{2lm}} |G|^{1-\frac{1}{l}-\frac{1}{m}}.$$

Estimates for T_k

D.R. Heath-Brown and S.V. Konyagin proved the following result, based on the method of S.A. Stepanov, the case $m = 2$; and S.V. Konyagin established for arbitrary m.

Theorem

For any m there is $C(m)$, such that for any p, G, and $t = |G| < p^{2/3}$ when $m = 2$ and $t = |G| < p^{1/2}$ when $m > 2$, there is the following estimate

$$T_m(G) \leq C(m)t^{2m-2+\frac{1}{2^m-1}}.$$

It allowed to obtain

Theorem

There is a function $C(\varepsilon) > 0$, such that if $|G| > p^{1/4+\varepsilon}$, then

$$|S(a, G)| = O(|G|p^{-C(\varepsilon)}).$$

Estimates for T_k

D.R. Heath-Brown and S.V. Konyagin proved the following result, based on the method of S.A. Stepanov, the case $m = 2$; and S.V. Konyagin established for arbitrary m.

Theorem

For any m there is $C(m)$, such that for any p, G, and $t = |G| < p^{2/3}$ when $m = 2$ and $t = |G| < p^{1/2}$ when $m > 2$, there is the following estimate

$$T_m(G) \le C(m) t^{2m-2+\frac{1}{2^m-1}}.$$

It allowed to obtain

Theorem

There is a function $C(\varepsilon) > 0$, such that if $|G| > p^{1/4+\varepsilon}$, then

$$|S(a, G)| = O(|G| p^{-C(\varepsilon)}).$$

Further progress

Yu.V. Malykhin obtained estimates for T_k and $|S(a, G)|$, in the case $G \subseteq (\mathbb{Z}/p^2\mathbb{Z})^*$ and proposed an approach for getting such estimates in $\mathbb{Z}/p^k\mathbb{Z}$.

J. Bourgain and S.V. Konyagin using combinatorial arguments deduced the followin.

Theorem

There exists a function $C(\varepsilon) > 0$, such that if $|G| > p^\varepsilon$, then

$$|S(a, G)| = O(|G| p^{-C(\varepsilon)}).$$

J. Bourgain obtained estimates of such type for arbitrary composite q.

Further progress

Yu.V. Malykhin obtained estimates for T_k and $|S(a, G)|$, in the case $G \subseteq (\mathbb{Z}/p^2\mathbb{Z})^*$ and proposed an approach for getting such estimates in $\mathbb{Z}/p^k\mathbb{Z}$.
J. Bourgain and S.V. Konyagin using combinatorial arguments deduced the followin.

Theorem

There exists a function $C(\varepsilon) > 0$, such that if $|G| > p^{\varepsilon}$, then

$$|S(a, G)| = O(|G|p^{-C(\varepsilon)}).$$

J. Bourgain obtained estimates of such type for arbitrary composite q.

Further progress

Yu.V. Malykhin obtained estimates for T_k and $|S(a, G)|$, in the case $G \subseteq (\mathbb{Z}/p^2\mathbb{Z})^*$ and proposed an approach for getting such estimates in $\mathbb{Z}/p^k\mathbb{Z}$.
J. Bourgain and S.V. Konyagin using combinatorial arguments deduced the followin.

Theorem

There exists a function $C(\varepsilon) > 0$, such that if $|G| > p^{\varepsilon}$, then

$$|S(a, G)| = O(|G| p^{-C(\varepsilon)}).$$

J. Bourgain obtained estimates of such type for arbitrary composite q.

futher progress

Theorem

(I. Shkredov) If $t = |G| \le \sqrt{p}$ then we have

$$T_2(G) = O(t^{\frac{5}{2} - C(\alpha)} (\log t)^{C'}),$$

where $C(\alpha) > 0$ and C' is some absolute, $t = p^{\alpha}$.

Theorem

(Iu.Sh., 2015) If $t = |G| \le \sqrt{p}$ then we have

$$T_3(G) = O(t^{4\frac{3}{14}} (\log t)^{C}),$$

where $C-$ is some absolute constant.

Theorem

(B. Murphy, M. Rudnev, I. Shkredov, Iu. Sh., arxiv.org)
If $t = |G| \le \sqrt{p}$ then we have

$$T_3(G) = O(t^4 \log t).$$

futher progress

Theorem

(I. Shkredov) If $t = |G| \leq \sqrt{p}$ then we have

$$T_2(G) = O(t^{\frac{5}{2} - C(\alpha)} (\log t)^{C'}),$$

where $C(\alpha) > 0$ and C' is some absolute, $t = p^{\alpha}$.

Theorem

(Iu.Sh., 2015) If $t = |G| \leq \sqrt{p}$ then we have

$$T_3(G) = O(t^{4\frac{3}{14}} (\log t)^{C}),$$

where $C-$ is some absolute constant.

Theorem

(B. Murphy, M. Rudnev, I. Shkredov, Iu. Sh., arxiv.org) If $t = |G| \leq \sqrt{p}$ then we have

$$T_3(G) = O(t^4 \log t).$$

futher progress

Theorem

(I. Shkredov) If $t = |G| \leq \sqrt{p}$ then we have

$$T_2(G) = O(t^{\frac{5}{2} - C(\alpha)} (\log t)^{C'}),$$

where $C(\alpha) > 0$ and C' is some absolute, $t = p^{\alpha}$.

Theorem

(Iu.Sh., 2015) If $t = |G| \leq \sqrt{p}$ then we have

$$T_3(G) = O(t^{4\frac{3}{14}} (\log t)^{C}),$$

where $C-$ is some absolute constant.

Theorem

(B. Murphy, M. Rudnev, I. Shkredov, Iu. Sh., arxiv.org)
If $t = |G| \leq \sqrt{p}$ then we have

$$T_3(G) = O(t^4 \log t).$$

Elements of the proof

Denote $r_3(a) = |\{(x_1, x_2, x_3) \in G^3 : x_1 - x_2 - x_3 = a\}|$.

$$T_3(G) = \sum_a r_3^2(a).$$

Consider the map $(u, v, w, z) \in G^4 \longrightarrow (uv, uz, wv)$. This is a surjective homomorphism of groups, kernel of which consists of $|G|$ elements.

$$r_3(a) = \frac{1}{|G|} \sum_{w,z} r_{(G-w)(G-z)}(a + wz),$$

where

$r_{(G-w)(G-z)}(l) = |\{(g_1, g_2) \in G^2 : (g_1 - w)(g_2 - z) = l\}|$.

Elements of the proof

Denote $r_3(a) = |\{(x_1, x_2, x_3) \in G^3 : x_1 - x_2 - x_3 = a\}|$.

$$T_3(G) = \sum_a r_3^2(a).$$

Consider the map $(u, v, w, z) \in G^4 \longrightarrow (uv, uz, wv)$. This is a surjective homomorphism of groups, kernel of which consists of $|G|$ elements.

$$r_3(a) = \frac{1}{|G|} \sum_{w,z} r_{(G-w)(G-z)}(a + wz),$$

where

$r_{(G-w)(G-z)}(l) = |\{(g_1, g_2) \in G^2 : (g_1 - w)(g_2 - z) = l\}|$.

Elements of the proof

Denote $r_3(a) = |\{(x_1, x_2, x_3) \in G^3 : x_1 - x_2 - x_3 = a\}|$.

$$T_3(G) = \sum_a r_3^2(a).$$

Consider the map $(u, v, w, z) \in G^4 \longrightarrow (uv, uz, wv)$. This is a surjective homomorphism of groups, kernel of which consists of $|G|$ elements.

$$r_3(a) = \frac{1}{|G|} \sum_{w,z} r_{(G-w)(G-z)}(a + wz),$$

where

$r_{(G-w)(G-z)}(l) = |\{(g_1, g_2) \in G^2 : (g_1 - w)(g_2 - z) = l\}|$.

Elements of the proof

Denote $r_3(a) = |\{(x_1, x_2, x_3) \in G^3 : x_1 - x_2 - x_3 = a\}|$.

$$T_3(G) = \sum_a r_3^2(a).$$

Consider the map $(u, v, w, z) \in G^4 \longrightarrow (uv, uz, wv)$. This is a surjective homomorphism of groups, kernel of which consists of $|G|$ elements.

$$r_3(a) = \frac{1}{|G|} \sum_{w,z} r_{(G-w)(G-z)}(a + wz),$$

where
$r_{(G-w)(G-z)}(l) = |\{(g_1, g_2) \in G^2 : (g_1 - w)(g_2 - z) = l\}|$.

Elements of the proof

$$T_3(G) = \frac{1}{|G|^2} \sum_a (\sum_{z,w} r_{(G-w)(G-z)}(a+wz))^2.$$

Using the Cauchy-Schwartz inequality we reduce previous expression to

$$\sum_{z,w} \sum_a r^2_{(G-w)(G-z)}(a+wz).$$

This is a number of solutions of equation

$$(u_1 - w)(v_1 - z) = (u_2 - w)(v_2 - z).$$

Points $(u_1, v_2), (w, z), (u_2, v_1)$ lie on the same line.
We are counting the number of collinear triples.
With the result of S.V. Konyagin (or D.A. Mitkin) based on Stepanov's method this quantity can be estimated.

Elements of the proof

$$T_3(G) = \frac{1}{|G|^2} \sum_a (\sum_{z,w} r_{(G-w)(G-z)}(a + wz))^2.$$

Using the Cauchy-Schwartz inequality we reduce previous expression to

$$\sum_{z,w} \sum_a r^2_{(G-w)(G-z)}(a + wz).$$

This is a number of solutions of equation

$$(u_1 - w)(v_1 - z) = (u_2 - w)(v_2 - z).$$

Points $(u_1, v_2), (w, z), (u_2, v_1)$ lie on the same line.
We are counting the number of collinear triples.
With the result of S.V. Konyagin (or D.A. Mitkin) based on Stepanov's method this quantity can be estimated.

Elements of the proof

$$T_3(G) = \frac{1}{|G|^2} \sum_a (\sum_{z,w} r_{(G-w)(G-z)}(a + wz))^2.$$

Using the Cauchy-Schwartz inequality we reduce previous expression to

$$\sum_{z,w} \sum_a r^2_{(G-w)(G-z)}(a + wz).$$

This is a number of solutions of equation

$$(u_1 - w)(v_1 - z) = (u_2 - w)(v_2 - z).$$

Points $(u_1, v_2), (w, z), (u_2, v_1)$ lie on the same line.
We are counting the number of collinear triples.
With the result of S.V. Konyagin (or D.A. Mitkin) based on Stepanov's method this quantity can be estimated.

Elements of the proof

$$T_3(G) = \frac{1}{|G|^2} \sum_a (\sum_{z,w} r_{(G-w)(G-z)}(a+wz))^2.$$

Using the Cauchy-Schwartz inequality we reduce previous expression to

$$\sum_{z,w} \sum_a r^2_{(G-w)(G-z)}(a+wz).$$

This is a number of solutions of equation

$$(u_1 - w)(v_1 - z) = (u_2 - w)(v_2 - z).$$

Points $(u_1, v_2), (w, z), (u_2, v_1)$ lie on the same line.
We are counting the number of collinear triples.
With the result of S.V. Konyagin (or D.A. Mitkin) based on Stepanov's method this quantity can be estimated.

Thank you for your attention