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:

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

This estimate corresponds to a trivial estimate for Gaussian sums

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

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 $|U| \leq CV$ 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

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

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 $\{u_1,\ldots,u_t\}$ and define its discrepancy as

$$\begin{aligned} D &= D_t(u_1,\ldots,u_t) \\ &= \sup_{0\le\alpha<\beta\le 1}\left|\frac{A([\alpha,\beta);t)}{t}-(\beta-\alpha)\right|, \end{aligned}$$

where $A([\alpha,\beta);t)=|\{j:\{u_j\}\in[\alpha,\beta)\}|$. Thus, D is small if the distribution of the sequence $\{u_1,\ldots,u_t\}$ 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 $\{u_1,\ldots,u_t\}=\{a_0x/p : x\in G\}$. 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

$$\begin{aligned} t(h+1)^2 &\le \sum_{a\in\mathbb{Z}_p^*} \left| \sum_{x\in G} \sum_{u,v=0}^{h} e(a(a_0 x - n - u + v)/p) \right| \\ &= \sum_{a\in\mathbb{Z}_p^*} \left| \sum_{x\in G} e(a a_0 x/p) \right| \left| \sum_{u=0}^{h} e(au/p) \right|^2 \\ &\le \eta t \sum_{a\in\mathbb{Z}_p^*} \left| \sum_{u=0}^{h} e(au/p) \right|^2 . \end{aligned} \tag{1.10}$$

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

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

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*

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

Then $T(p) \leq t_0$.

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

$$pN = \sum_{x_1,\ldots,x_d \in G} \sum_{a \in \mathbb{Z}_p} e\left(a \sum_{j=1} b_j x_j / p\right)$$

$$= \sum_{a \in \mathbb{Z}_p} \prod_{j=1}^{d} \sum_{x_j \in G} e(ab_j x_j / p)$$

$$= \sum_{a \in \mathbb{Z}_p} \prod_{j=1}^{d} S(ab_j, G). \tag{1.14}$$

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

$$|pN - |G|^d| = \left| \sum_{a \in \mathbb{Z}_p^*} \prod_{j=1}^{d} S(ab_j, G) \right|$$

$$\leq (p-1) \left(\max_{a \in \mathbb{Z}_p^*} |S(a, G)| \right)^d,$$

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*

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

Proof. By Lemma 1.6 and Lemma 1.2, we get

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

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

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

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*

$$(1.16) \qquad |G| \leq u \log p$$

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

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

and

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

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

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

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*

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

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

$$\begin{aligned} t|S(a_0, G)|^{2k} &= \sum_{x \in G} |S(a_0 x, G)|^2 \\ &\leq \sum_{a \in G} |S(a, G)|^{2k} = pT_k(G), \end{aligned}$$

and the proposition follows.

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

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

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

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

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