New bounds for Heilbronn’s exponential sum *

Shkredov I.D.

Annotation.

Using Stepanov’s method and some combinatorial observations we prove a new upper bound for Heilbronn’s exponential sum and obtain a series of applications of our result to distribution of Fermat quotients.

1 Introduction

Let $p$ be a prime number. Heilbronn’s exponential sum is defined by

$$S(a) = \sum_{n=1}^{p} e^{2\pi i \cdot \frac{an}{p^2}}. \quad (1)$$

D.R. Heath–Brown obtained in [4] the first nontrivial upper bound for the sum. After that the result was improved in papers [5], [15] (see also [21]). Let us formulate, for example, the main result from [15].

**Theorem 1** Let $p$ be a prime, and $a \not\equiv 0 \pmod{p}$. Then

$$|S(a)| \ll p^{0.36} \log^{0.5} p.$$ 

The main result of the paper is the following.

**Theorem 2** Let $p$ be a prime, and $a \not\equiv 0 \pmod{p}$. Then

$$|S(a)| \ll p^{0.31} \log^{0.5} p.$$ 

---

*This work was supported by grant RFFI NN 11-01-00759, Russian Government project 11.G34.31.0053, Federal Program "Scientific and scientific–pedagogical staff of innovative Russia" 2009–2013, grant mol 겱 뜘 12–01–33080 and grant Leading Scientific Schools N 2519.2012.1.
Heilbronn’s exponential sum is connected (see e.g. [1], [2], [7], [10], [17], [18]) with so-called Fermat quotients defined as

\[ q(n) = \frac{n^{p-1} - 1}{p}, \quad n \neq 0 \pmod{p}. \]

Our main result has some applications to the distribution of such quotients. The list of the applications can be found in [15] (see also section 4).

Our approach can be described as follows. Clearly, sum (1) can be considered as the sum over the following multiplicative subgroup

\[ \Gamma = \{ m^p : 1 \leq m \leq p - 1 \} \subseteq \mathbb{Z}/(p^2\mathbb{Z}) \]  \hspace{1cm} (2)

(see the discussion at the beginning of section 3). Recently, some progress in estimating of exponential sums over ”large” subgroups (but in \( \mathbb{Z}/p\mathbb{Z} \) not in \( \mathbb{Z}/p^2\mathbb{Z} \)) such as (2) was attained (see [14]). So, it is natural to try to use the approach from the paper to obtain a new upper bound for (1). Applying Stepanov’s method (see section 3) as well as some combinatorial observations (see Lemma 11), we estimate ”the additive energy” of the subgroup \( \Gamma \). This new bound easily implies our main Theorem 2.

We are going to obtain some new facts about distribution of the elements of the group \( \Gamma \) in the future.

The author is grateful to Sergey Konyagin for useful discussions.

## 2 Definitions

Let \( G \) be an abelian group. If \( G \) is finite then denote by \( N \) the cardinality of \( G \). It is well-known [11] that the dual group \( \hat{G} \) is isomorphic to \( G \) in the case. Let \( f \) be a function from \( G \) to \( \mathbb{C} \). We denote the Fourier transform of \( f \) by \( \hat{f} \),

\[ \hat{f}(\xi) = \sum_{x \in G} f(x)e(-\xi \cdot x), \]  \hspace{1cm} (3)

where \( e(x) = e^{2\pi i x} \). If

\[ (f * g)(x) := \sum_{y \in G} f(y)g(x - y) \quad \text{and} \quad (f \circ g)(x) := \sum_{y \in G} f(y)g(y + x) \]

then

\[ \hat{f} * \hat{g} = \hat{f} \hat{g} \quad \text{and} \quad \hat{f} \circ \hat{g} = \hat{f}^{\circ} \hat{g} = \overline{\hat{g}}, \]  \hspace{1cm} (4)

where for a function \( f : G \to \mathbb{C} \) we put \( f^*(x) := f(-x) \). Clearly, \( (f * g)(x) = (g * f)(-x) \) and \( (f \circ g)(x) = (g \circ f)(-x), x \in G \). The \( k \)-fold convolution, \( k \in \mathbb{N} \) we denote by \( *_k \), so \( *_k := *_{k-1} \).

We use in the paper the same letter to denote a set \( S \subseteq G \) and its characteristic function \( S : G \to \{0,1\} \). Write \( E(A,B) \) for the additive energy of two sets \( A, B \subseteq G \) (see e.g. [20]), that is

\[ E(A,B) = |\{a_1 + b_1 = a_2 + b_2 : a_1, a_2 \in A, b_1, b_2 \in B\}|. \]
If $A = B$ we simply write $E(A)$ instead of $E(A, A)$. Clearly,

$$E(A, B) = \sum_x (A \ast B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x)(B \circ B)(x).$$  \hfill (5)

Put for any $A \subseteq G$

$$T_k(A) := |\{a_1 + \cdots + a_k = a'_1 + \cdots + a'_k \ : \ a_1, \ldots, a_k, a'_1, \ldots, a'_k \in A\}|.$$

Let

$$E_k(A) = \sum_{x \in G} (A \circ A)(x)^k,$$

and

$$E_k(A, B) = \sum_{x \in G} (A \circ A)(B \circ B)(x)^{k-1}$$

be the higher energies of $A$ and $B$. Similarly, we write $E_k(f, g)$ for any complex functions $f$ and $g$. Quantities $E_k(A, B)$ can be expressed in terms of generalized convolutions (see [13]).

**Definition 3** Let $k \geq 2$ be a positive number, and $f_0, \ldots, f_{k-1} : G \to \mathbb{C}$ be functions. Write $F$ for the vector $(f_0, \ldots, f_{k-1})$ and $x$ for vector $(x_1, \ldots, x_{k-1})$. Denote by $C_k(f_0, \ldots, f_{k-1})(x_1, \ldots, x_{k-1})$ the function

$$C_k(F)(x) = C_k(f_0, \ldots, f_{k-1})(x_1, \ldots, x_{k-1}) = \sum_z f_0(z)f_1(z+x_1)\cdots f_{k-1}(z+x_{k-1}).$$

Thus, $C_2(f_1, f_2)(x) = (f_1 \circ f_2)(x)$. If $f_1 = \cdots = f_k = f$ then write $C_k(f_1, \ldots, f_k)(x_1, \ldots, x_{k-1})$ for $C_k(f)(x_1, \ldots, x_{k-1})$.

For a positive integer $n$, we set $[n] = \{1, \ldots, n\}$. All logarithms used in the paper are to base 2. By $\ll$ and $\gg$ we denote the usual Vinogradov’s symbols. If $N$ is a positive integer then write $\mathbb{Z}_N$ for $\mathbb{Z}/N\mathbb{Z}$ and $\mathbb{Z}_N^*$ for the subgroup of all invertible elements of $\mathbb{Z}_N$.

## 3 Stepanov’s method

Let $p$ be a prime number, $p \geq 3$. Put

$$\Gamma = \{m^p \ : \ 1 \leq m \leq p - 1\} \subseteq \mathbb{Z}_{p^2}.$$

It is easy to see that $\Gamma$ is a subgroup and that

$$\Gamma = \{x^p \ : \ x \in \mathbb{Z}_{p^2}^*\} = \{x \in \mathbb{Z}_{p^2}^* \ : \ x^{p-1} \equiv 1 \pmod{p^2}\}$$

because of $x \equiv y \pmod{p}$ implies $x^p \equiv y^p \pmod{p^2}$. Further, one can check

$$\mathbb{Z}_{p^2}^* = \bigsqcup_{j=1}^p (1 + pj)\Gamma := \bigsqcup_{j=1}^p \xi_j \Gamma,$$
and \( \mathbb{Z}_p^2 \setminus \mathbb{Z}_p^* = \{0\} \cup p\Gamma \) (see [8]).

Put

\[
f(x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots + \frac{x^{p-1}}{p-1} \in \mathbb{Z}_p[X].
\]

Recall a lemma from [8].

**Lemma 4** Let \( r \geq 2 \) be a positive integer, and \( R \subseteq \mathbb{Z}_p^r \) be a multiplicative subgroup, \( |R| \) divides \( p-1 \). Then the natural projection \( \varphi : \mathbb{Z}_p^r \to \mathbb{Z}_p^{r-1} \) is a bijection onto \( R \) and \( \varphi(R) \) is a multiplicative subgroup of \( \mathbb{Z}_p^{r-1} \) (of size \( |R| \)).

We need in a simple lemma.

**Lemma 5** Let \( \lambda = (1 + sp)g, s \in [p] \) and \( g \in \Gamma \). For all \( i, j \in [p] \) the following holds

\[
|\{x - y \equiv \lambda \pmod{p^2} : x \in \xi_i\Gamma, y \in \xi_j\Gamma\}| = |\{b \in \mathbb{Z}_p : f(bg^{-1} \pmod{p}) \equiv (i-j)bg^{-1} + j-s\}|.
\]

Further

\[
|\{x - y \equiv \lambda \pmod{p^2} : x \in \xi_i\Gamma, y \in p\Gamma\}| \leq 1,
\]

and

\[
|\{x - y \equiv \lambda \pmod{p^2} : x \in p\Gamma, y \in \xi_j\Gamma\}| \leq 1.
\]

**Proof.** Let us prove (8). For some \( 1 \leq m, n \leq p-1 \), we have

\[
x - y \equiv (1 + pi)m^p - (1 + pj)n^p \equiv \lambda \pmod{p^2}.
\]

Thus \( n \equiv m - g \pmod{p} \) and we obtain

\[
(1 + pi)m^p - (1 + pj)n^p \equiv (1 + pi)m^p - (1 + pj)(m - g)^p \equiv \sum_{l=1}^{p} (-1)^{l-1} \binom{p}{l} g^l m^{p-l} + p(im - j(m - g))
\]

\[
\equiv g - pgf(mg^{-1}) + p(im - j(m - g)) \equiv \lambda \pmod{p^2}
\]

as required. In formula (11) we have used the fact that \( g \in \Gamma \) and hence \( g^{p-1} \equiv 1 \pmod{p^2} \).

Further, suppose that for \( m, n \) such that \( 1 \leq m, n \leq p-1 \) the following holds

\[
(1 + pi)m^p - pn^p \equiv \lambda \pmod{p^2}.
\]

Then \( m \equiv g \pmod{p} \) and hence by Lemma 4 the number \( m \) is determined uniquely. Substitution \( m \) into (12) gives us \( n \equiv (i-s)g \pmod{p} \). Such \( n \) does not exists if \( (i-s) \equiv 0 \pmod{p} \) and \( n \) is determined uniquely otherwise. So, we have obtained (9). Inequality (10) follows similarly.

This completes the proof. \( \square \)

Denote the sets from (8) as \( M_{i,j}(\lambda) \) and from (9), (10) as \( M_{i,0}(\lambda), M_{0,j}(\lambda) \), correspondingly. Thus the previous lemma represents the sizes of such sets from \( \mathbb{Z}_p^2 \) via the sizes of some sets in \( \mathbb{Z}_p^r \). If \( \lambda = 1 \) then we write just \( M_{i,j}, M_{i,0}, \) and \( M_{0,j} \).

To use Stepanov’s method we need in a lemma from [4].
Lemma 6 Let \( r \) be a positive integer. Then there are two polynomials \( q_r(X), h_r(X) \in \mathbb{Z}_p[X] \) such that \( \deg q_r \leq r + 1, \deg h_r \leq r - 1 \) and

\[
(X(1 - X))^r \left( \frac{d}{dX} \right)^r f(X) = q_r(X) + (X^p - X)h_r(X).
\]

Thus we can convert the polynomial \( f(X) \) of large degree (and its derivatives) into \( q_r(X) \), which has small degree. Also we need in a lemma on linear independence of some family of polynomials.

Lemma 7 Let \( F(X,Y) \in \mathbb{Z}_p[X,Y] \) have degree less then \( A \) with respect to \( X \), and degree less then \( B \) with respect to \( Y \). Suppose that \( AB \leq p \) and \( F \) is not vanish identically. Then \( X^p \) does not divide \( F(X,f(X)) \).

Now we formulate the main result of the section. We use Stepanov’s method \([19],[4],[5],[6]\) in the proof.

Proposition 8 Suppose that \( Q,Q_1,Q_2 \subseteq \mathbb{Z}_p^* \) are \( \Gamma \)-invariant sets and \( |Q||Q_1||Q_2| \ll p^5 \). Then

\[
\sum_{x \in Q} (Q_1 \circ Q_2)(x) \ll p^{-1/3}(|Q||Q_1||Q_2|)^{2/3}.
\]  \hspace{1cm} (13)

Proof. Let \( s = |Q||Q_1||Q_2|/|\Gamma|^3 \). Clearly, \( s \) is a positive integer. By Lemma 5 (one can take the parameter \( \lambda \) equals 1) to estimate the sum from (13) we need to find an appropriate upper bound for the size of the following set

\[
M := \bigcup_{l=1}^s M_{i,l,j}.
\]

Consider a polynomial \( \Phi \in \mathbb{Z}_p[X,Y,Z] \) such that

\[
\deg_X \Phi < A, \quad \deg_Y \Phi < B, \quad \deg_Z \Phi < C.
\]

We have

\[
\Phi(X,Y,Z) = \sum_{a,b,c} \lambda_{a,b,c} X^a Y^b Z^c.
\]  \hspace{1cm} (14)

Besides take

\[
\Psi(X) = \Phi(X,f(X),X^p).
\]  \hspace{1cm} (15)

Clearly

\[
\deg \Psi < A + p(B + C).
\]

If we will find the coefficients \( \lambda_{a,b,c} \) such that, firstly, the polynomial \( \Psi \) is nonzero, and, secondly, \( \Psi \) has a root of order at least \( D \) at any point of the set \( M \) (except 0 and 1, may be) then

\[
|M| \ll (A + p(B + C))/D
\]  \hspace{1cm} (16)
Thus, we should check that
\[
\left. \left( \frac{d}{dX} \right)^n \Psi(X) \right|_{X=x} = 0, \quad \forall n < D, \quad \forall x \in M.
\]
It is easy to see that for all \(m, q, q \geq m\), and any \(\mu\) the following holds
\[
(X - \mu)^m \left( \frac{d}{dX} \right)^m (X - \mu)^q = \frac{q!}{(q - m)!} (X - \mu)^q.
\]
If \(m > q\) then the left hand side equals zero. Using the last formula and Lemma 6 it is easy to check (or see [4], [8]) that for any \(x \in M\),
\[
[X(1 - X)]^n \left( \frac{d}{dX} \right)^n X^a f(X)^b X^{cp} \bigg|_{X=x} = P_{n,l,a,b,c}(x),
\]
where \(P_{n,l,a,b,c}(X)\) is a polynomial of degree at most \(A + B + C + 2D\). Whence for any \(x \in M\), we have
\[
[X(1 - X)]^n \left( \frac{d}{dX} \right)^n \Psi(X) \bigg|_{X=x} = P_{n,l}(x),
\]
and each polynomial \(P_{n,l}\) has at most \(A + B + C + 2D\) coefficients, which are linear forms of \(\lambda_{a,b,c}\). Thus if
\[
sD(A + B + C + 2D) < ABC
\]
then there are coefficients \(\lambda_{a,b,c}\) not all zero such that the polynomials \(P_{n,l}\) vanish for all \(n < D\) and all \(l \in [s]\).

We choose the parameters \(A, B, C\) and \(D\) as
\[
A = \left[p^{2/3}s^{-1/3}\right], \quad B = C = \left[p^{1/3}s^{1/3}\right], \quad D = \left[p^{2/3}s^{-1/3}/32\right].
\]
The assumption \(|Q_1||Q_2| < p^5\) implies that \(s < p^2\) and hence the choice is admissible. Quick calculations show that the parameters satisfy condition (17). Further, we have \(AB \leq p\) and by Lemma 7 our polynomial \(\Psi\) does not vanish identically. Finally, substitution of the parameters into (16) gives the required bound. This completes the proof. \(\square\)

Previous versions of the result above can be found in [4], [5]. Variants for other groups are contained in [6], [8].

Using Proposition 8 one can easily deduce upper bounds for moments of convolution of \(\Gamma\). These estimates are the same as in the case of multiplicative subgroups in \(\mathbb{Z}_p\) (see, e.g. [12]).

**Corollary 9** We have
\[
E(\Gamma) \ll |\Gamma|^{5/2}, \quad E_3(\Gamma) \ll |\Gamma|^3 \log |\Gamma|, \quad (18)
\]
and for all \(l \geq 4\) the following holds
\[
E_l(\Gamma) = |\Gamma|^l + O(|\Gamma|^{2l/3}) \quad (19)
\]
The same method gives a generalization (see the analogous proof in \[6\]). Actually, one can takes different cosets of $\Gamma$ in theorem below.

**Theorem 10** Let $d \geq 2$ be a positive integer. Arranging $(\Gamma *_{d-1} \Gamma)(\xi_1) \geq (\Gamma *_{d-1} \Gamma)(\xi_2) \geq \ldots$, where $\xi_j \neq 0$ belong to distinct cosets, we have

$$(\Gamma *_{d-1} \Gamma)(\xi_j) \ll_d |\Gamma|^{d-2+3^{-1} (1+2^{2^d-1})} \cdot j^{-\frac{1}{3}}.$$  

In particular

$$T_d(\Gamma) \ll_d |\Gamma|^{2d-2+2^{1-d}}, \quad (20)$$

further

$$\sum \langle \Gamma \circ_{d-1} \Gamma \rangle^3(z) \ll_d |\Gamma|^{3d-4+2^{2-d}} \cdot \log |\Gamma|, \quad (21)$$

and similar

$$\sum \langle \Gamma \circ \Gamma \rangle (z) \langle (\Gamma *_{d-1} \Gamma) \circ (\Gamma *_{d-1} \Gamma) \rangle^2(z) \ll_d |\Gamma|^{4d-2+3^{-1} (1+2^{2^d-2d})} \cdot \log |\Gamma|. \quad (22)$$

4 The proof of the main result

We formulate Proposition 28 from \[14\]. This is a key new ingredient of our proof.

**Lemma 11** Let $A \subseteq G$ be a set, and let $\psi$ be a real even function with $\hat{\psi} \geq 0$. Then

$$\frac{1}{|A|^3} \left( \sum_x \psi(x)(A \circ A)(x) \right)^3 \leq \sum_{x,y,z \in A} \psi(x-y)\psi(x-z)\psi(y-z).$$

Now we can prove our main result.

**Theorem 12** Let $p$ be a prime number. Then

$$E(\Gamma) \ll p^{\frac{2}{3}} \log^2 p. \quad (23)$$

and, more generally, for all $k \geq 2$, we have

$$T_k(\Gamma) \ll_k p^{2k-\frac{17}{3} + \frac{15}{3} 2^{-2k}} \log^2 p. \quad (24)$$
Proof. Let $|\Gamma| = t = p - 1$, $E_3(\Gamma) = E_3$, $T_l = T_l(\Gamma)$, $l \geq 2$. Put

$$\psi = \psi_k(x) = ((\Gamma *_{k-1} \Gamma) \circ (\Gamma *_{k-1} \Gamma))(x)$$

for $k \geq 1$. Obviously, $\hat{\psi} \geq 0$ and $\psi$ is an even function. By Lemma 11, we have

$$\sum_{x,y,z \in \Gamma} \psi(x - y)\psi(x - z)\psi(y - z) \geq \frac{T_{k+1}^3}{t^3}.$$  \hspace{1cm} (25)

In other words

$$\sum_{\alpha,\beta} \psi(\alpha)\psi(\beta)\psi(\alpha - \beta)C_3(\Gamma)(\alpha, \beta) \geq \frac{T_{k+1}^3}{t^3}.$$  \hspace{1cm} (26)

Clearly,

$$\sum_{\alpha \neq 0, \beta \neq 0, \alpha \neq \beta} \psi(\alpha)\psi(\beta)\psi(\alpha - \beta)C_3(\Gamma)(\alpha, \beta) \geq \frac{T_{k+1}^3}{2t^3}.$$  \hspace{1cm} (27)

because if $\alpha, \beta$ or $\alpha - \beta$ equals zero then by Theorem 10, we get

$$\frac{t^{6k-4+3^{-1}(1+2^{3-2k})+2^{-1-k}} \log t}{t} \gg T_k(\Gamma) \cdot \sum_x \psi^2(x)(\Gamma \circ \Gamma)(x) \gg t^{-3}T_{k+1}^3(\Gamma)$$

and the result follows. Further, the summation in (26) can be taken over nonzero $\alpha$ such that

$$\psi(\alpha) \geq 2^{-4} \frac{T_{k+1}}{t^2} := d.$$ \hspace{1cm} (28)

Here we have used the subgroup property which implies that

$$\sum_{x \in \Gamma} (\psi * \Gamma)^2(x) = t^{-1} \left( \sum_x \psi(x)(\Gamma \circ \Gamma)(x) \right)^2.$$ \hspace{1cm} (29)

Applying the Cauchy–Schwartz inequality one more time, we obtain

$$\sum_{\alpha \neq 0, \beta \neq 0, \alpha \neq \beta : \psi(\alpha), \psi(\beta), \psi(\alpha - \beta) \gg d} \psi^2(\alpha)\psi^2(\beta)\psi^2(\alpha - \beta) \gg t^{-6}T_{k+1}^6(\Gamma) \cdot E_3^{-1}.$$ \hspace{1cm} (30)

because of

$$\sum_{\alpha, \beta} C_3^2(\Gamma)(\alpha, \beta) = E_3.$$  \hspace{1cm} (31)

Put

$$S_i = \{ x \in \Gamma - \Gamma, x \neq 0 : 2^{i-1}d < \psi(x) \leq 2^id \}, \quad i \in [l], \quad l \ll \log t.$$  \hspace{1cm} (32)

Then

$$d^6 \cdot \sum_{i,j,k=1}^l 2^{2i+2j+2k} \sum_{\alpha} S_i(\alpha)(S_j \ast S_k)(\alpha) \gg t^{-6}T_{k+1}^6(\Gamma) \cdot E_3^{-1}.$$  \hspace{1cm} (33)

because of

$$\sum_{\alpha} C_3^2(\Gamma)(\alpha, \beta) = E_3.$$  \hspace{1cm} (34)
To estimate the inner sum in (30) we use Proposition 8. First of all, note that by Theorem 10 or Proposition 8 one has

$$|S_i| \ll t^{6k-4+2^{-2k}2-3i}d^{-3}.$$  

(31)

Using the last estimate it is easy to see that for all $i, j, k \in \mathbb{Z}$ the following inequality holds

$$|S_i||S_j||S_k| \ll (t^{6k-4+2^{-2k}2-3i}d^{-3})^3 \ll t^{18k-12+122^{-2k}d^{-9}} = t^{18k+6+122^{-2k}T_{k+1}^{-9}} \ll p^5$$

(32)

because otherwise bound (24) takes place. Then by Proposition 8

$$d^6p^{-1/3} \sum_{i,j,k=1}^l 2^{2i+2j+2k}(|S_i||S_j||S_k|)^{2/3} \gg t^{-6}T_{k+1}^6(\Gamma) : E_3^{-1}.$$

Hence, using inequality (31) once again, we get

$$t^{12k-8+2^{-2k}-1/3} \log^3 t \gg t^{-6}T_{k+1}^6(\Gamma) : E_3^{-1}.$$  

(33)

Inequality (33) implies that

$$T_{k+1} \ll t^{2k+1/9+2^{-2k}/3} \log^{2/3} t$$

and we are done. This completes the proof.

Thus, inequality (31) is better then bound (20) of Theorem 10 for $k = 2$ and for $k = 3$, namely, $T_3(\Gamma) \ll t^{151/36} \log^{2/3} t$. Using more accurate arguments from [6] one can, certainly, improve our bounds for large $k$. We do not make such calculations.

**Remark 13** To obtain (28) we have used the fact that $\Gamma$ is a subgroup. For general set $A$ a similar inequality takes place. Indeed, let $g$ be a real even function and $A$ be a set. In terms of paper [10] (or see [14]), we have $(T_A^g)^2(x, y) = C_3(A^c, g, g)(x, y)$ and, hence,

$$\mu_0^2(T_A^g) \geq |A|^{-1} \langle (T_A^g)^2, A, A \rangle = |A|^{-1} \sum_{x \in A} (A * g)(x).$$

Thus, the arguments in lines (26)–(29) take place in general.

Theorem above implies a result on exponential sums over subgroups in $\mathbb{Z}_{p^2}^*$ (see details of the proof in [11] or [15]).

**Corollary 14** Let $p$ be a prime, $a \neq 0 \pmod{p}$, and $M, N$ be positive integers, $N \leq p$. Then

$$\left| \sum_{n=M}^{N+M} e\left(\frac{anp}{p^2}\right) \right| \ll p^{11/2} N^{1/4} \log^{1/2} p.$$  

(34)

In particular

$$|S(a)| \ll p^{3/4} \log^{3/4} p.$$  

(35)
Sketch of the proof. We have
\[ |S(a)| \leq E^{1/4}(\Gamma)N^{1/4} \]
and the result follows. □

Using the arguments from [1] and Theorem 12, we obtain the following result about Fermat quotients. By \( l_p \) denote the smallest \( n \) such that \( q(n) \neq 0 \pmod{p} \). In [1] an upper bound for \( l_p \) was obtained.

Theorem 15 One has
\[ l_p \leq (\log p)^{461/252 + o(1)} \]
as \( p \to \infty \).

In [15] we found an estimate for the additive energy of \( \Gamma \) which allows improve Theorem 15. Namely, we got
\[ l_p \leq (\log p)^{7829/4284 + o(1)} \]

Now we formulate our new result on upper bound for \( l_p \).

Theorem 16 One has
\[ l_p \leq (\log p)^{131/72 + o(1)} \]
as \( p \to \infty \).

Sketch of the proof. Let \( l_p = (\log p)^{\kappa + o(1)} \), \( \kappa > 0 \). Let also \( k < p^2 \) be a positive integer and put \( N(k) \) be the number solutions of the congruence
\[ ux \equiv y, \quad 0 < |x|, |y| \leq p^{2+o(1)}k^{-1}, \quad u \in \Gamma. \]
By the arguments of paper [1] the number \( \kappa \) can be estimated, very roughly, from the formula
\[ k = p^\kappa, \quad \text{where } k \text{ is the smallest number such that inequality} \]
\[ \frac{k}{p} \gg \frac{k}{p^3} \left( \frac{p^9E(\Gamma)N(k)}{k^2} \right)^{1/4} \quad (36) \]
holds. To estimate \( N(k) \) we use Lemma 9 from [1] which gives for any positive integer \( \nu \) that
\[ N(k) \ll (p^{2+o(1)}k^{-1})p^{1/(2\nu(\nu+1))} + (p^{2+o(1)}k^{-1})^2p^{-1/\nu}. \]
Choosing \( \nu = 6 \), we find in the range of parameter \( k \) that
\[ N(k) \ll (p^{2+o(1)}k^{-1})^2p^{-1/6}. \]
Substituting the last estimate into (36), we obtain the result. □

Note that
\[ \frac{7829}{4284} = 1.82749 \ldots \quad \text{and} \quad \frac{131}{72} = 1.81944 \ldots. \]
It was conjectured by A. Granville (see [3], Conjecture 10) that
\[ l_p = o((\log p)^\frac{1}{4}) \]
and H. W. Lenstra [7] conjectured that, actually, \( l_p \leq 3 \).

Theorem 16 has a consequence (see [7]).

**Corollary 17** For every \( \epsilon > 0 \) and a sufficiently large integer \( n \), if \( a^{n-1} \equiv 1 \pmod{n} \) for every positive integer \( a \leq (\log p)^{\frac{131}{72}+\epsilon} \) then \( n \) is squarefree.

Discussion and further applications can be found in [15].

5 Concluding remarks

At the end of the paper we make a several remarks about possible extensions of our results onto the groups \( \mathbb{Z}_{p^k}^* \), \( k \geq 1 \).

We begin with the problem of estimation of exponential sums over multiplicative subgroups of such groups. It can be shown (see [9]) that if \( \Gamma \subseteq \mathbb{Z}_{p^k}^* \) is a subgroup and \( p \) divides \( |\Gamma| \) then the exponential sum over \( \Gamma \) vanishes. Thus a question about the estimation of exponential sums is trivial in the case. If \( |\Gamma| \) divides \( p-1 \) then the exponential sum can be reduced to the cases of subgroups in \( \mathbb{Z}_p^* \) and \( \mathbb{Z}_{p^2}^* \) (see the main result from [9]). The reason is the existence of the natural projection \( \varphi : \mathbb{Z}_{p^k}^* \rightarrow \mathbb{Z}_{p^{k-1}}^* \), \( k \geq 2 \) which is defined by the rule \( \varphi(x) \equiv x \pmod{p^{k-1}} \), see Lemma 4.

The projection \( \varphi \) allows estimate quantities \( T_l(\Gamma), \Gamma \subseteq \mathbb{Z}_{p^k}^* \) via quantities \( T_l(\varphi(\Gamma)) \) of subgroups from \( \mathbb{Z}_{p^{k-1}}^* \). In \( \mathbb{Z}_{p^2}^* \) an adaptation of Stepanov’s method from [8] gives such estimates directly, provided by \( |\Gamma| \) divides \( p-1 \). The existence of Stepanov’s estimates similar Proposition 8 allows to apply the method from section 4 to obtain better bounds. We do not make such calculations.

References

[1] J. Bourgain, K. Ford, S. V. Konyagin, I. E. Shparlinski, *On the Divisibility of Fermat Quotients*, Michigan Math. J. 59 (2010), 313–328.

[2] M.-C. Chang, *Short character sums with Fermat quotients*, Acta Arith. 152 (2012), 23–38.

[3] A. Granville, *Some conjectures related to Fermat’s Last Theorem*, Number Theory W. de Gruyter, NY, 1990, 177–192.

[4] D. R. Heath–Brown, *An estimate for Heilbronn’s exponential sum*, Analytic number theory vol. 2, (Allerton Park, IL 1995), Progr. Math., 1 39, Birkhäuser, Boston (1996), 451–463.
D. R. Heath–Brown, S. V. Konyagin, \textit{New bounds for Gauss sums derived from \(k\)th powers, and for Heilbronn's exponential sum}, Quart. J. Math. \textbf{51} (2000), 221–235.

S. V. Konyagin, \textit{Estimates for trigonometric sums and for Gaussian sums // IV International conference ”Modern problems of number theory and its applications”. Part 3} (2002), 86–114.

H. W. Lenstra, \textit{Miller’s primality test}, Inform. Process. Lett. \textbf{8} (1979), 86–88.

Yu. V. Malykhin, \textit{Bounds for exponential sums over \(p^2\)}, Journal of Mathematical Sciences \textbf{146}:2 (2007), 5686–5696.

Yu. V. Malykhin, \textit{Bounds for exponential sums over \(p^k\)}, Math. Notes (2006), 793–796.

A. Ostafe, I. E. Shparlinski, \textit{Pseudorandomness and dynamics of Fermat quotients}, SIAM J. Discr. Math. \textbf{25} (2011), 50–71.

W. Rudin, \textit{Fourier analysis on groups}, Wiley 1990 (reprint of the 1962 original).

T. Schoen, I. D. Shkredov, \textit{Additive properties of multiplicative subgroups of \(\mathbb{F}_p\)}, Quart. J. Math. \textbf{63}:3 (2012), 713–722.

T. Schoen, I. D. Shkredov, \textit{Higher moments of convolutions}, J. of Number Theory, \textbf{133} (2013), 1693–1737.

I. D. Shkredov, \textit{Some new inequalities in additive combinatorics}, \texttt{arXiv:1208.2344v3 [math.CO]} 6 Nov 2012.

I. D. Shkredov, \textit{On Heilbronn’s exponential sum}, Quart. J. Math., doi: 10.1093/qmath/has037.

I. D. Shkredov, \textit{Some new results on higher energies}, \texttt{arXiv:1212.6414v1 [math.CO]} 27 Dec 2012.

I. E. Shparlinski, \textit{On the value set of Fermat quotients}, Proc. Amer. Math. Soc. \textbf{140} (2012), 1199–1206.

I. E. Shparlinski, \textit{On vanishing Fermat quotients and a bound of the Ihara sum}, Kodai Math. J. (to appear), \texttt{arXiv:1104.3910v1 [math.NT]}.

S. A. Stepanov, \textit{On the number of points on hyperelliptic curve over prime finite field}, IAN \textbf{33} (1969), 1171–1181.

T. Tao, V. Vu, \textit{Additive combinatorics}, Cambridge University Press 2006.

H. B. Yu, \textit{Note on Heath–Brown estimate for Heilbronn’s exponential sum}, Proc. AMS \textbf{127}:7 (1999), 1995–1998.
Division of Algebra and Number Theory,
Steklov Mathematical Institute,
ul. Gubkina, 8, Moscow, Russia, 119991
and
Delone Laboratory of Discrete and Computational Geometry,
Yaroslavl State University,
Sovetskaya str. 14, Yaroslavl, Russia, 150000
and
IITP RAS,
Bolshoy Karetny per. 19, Moscow, Russia, 127994

ilya.shkredov@gmail.com