On tripling constant of multiplicative subgroups *

Shkredov I.D.

Annotation. We prove that any multiplicative subgroup \( \Gamma \) of the prime field \( \mathbb{F}_p \) with \( |\Gamma| < \sqrt{p} \) satisfies \( |3\Gamma| \gg \frac{|\Gamma|^2}{\log |\Gamma|} \). Also, we obtain a bound for the multiplicative energy of any nonzero shift of \( \Gamma \), namely \( E^\times(\Gamma + x) \ll |\Gamma|^2 \log |\Gamma| \), where \( x \neq 0 \) is arbitrary.

1 Introduction

Let \( p \) be a prime number, \( \mathbb{F}_p \) be the finite field, and \( \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\} \). Let also \( \Gamma \subseteq \mathbb{F}_p^* \) be an arbitrary multiplicative subgroup. Such subgroups were studied by various authors (see the references in [6]). One of the interesting question is the determination of the additive structure of multiplicative subgroups, see e.g. [11, 2, 3, 4, 9, 10, 11, 13]. In particular, what can we say about the size of sumsets of subgroups, that is about the sets of the form

\[
2\Gamma = \Gamma + \Gamma := \{\gamma_1 + \gamma_2 : \gamma_1, \gamma_2 \in \Gamma\}?
\]

There is a well–known conjecture that the sumset \( 2\Gamma \) contains \( \mathbb{F}_p^* \), provided that \( |\Gamma| > p^{1/2+\varepsilon} \), where \( \varepsilon > 0 \) is any number and \( p \geq p(\varepsilon) \) is large enough. In the article we study a bigger set \( 3\Gamma = \Gamma + \Gamma + \Gamma \) instead of \( 2\Gamma \). Let us formulate the main result of the paper.

**Theorem 1** Let \( p \) be a prime number, \( \Gamma \subset \mathbb{F}_p^* \) be a multiplicative subgroup, \( |\Gamma| < \sqrt{p} \). Then

\[
|3\Gamma| \gg \frac{|\Gamma|^2}{\log |\Gamma|}.
\]

It is interesting to compare Theorem 1 with a result of A.A. Glibichuk who obtained in [3] that \( |4\Gamma| > p/2 \) provided \( |\Gamma| > \sqrt{p} \) as well as with a result from [11] : \( \mathbb{F}_p^* \subseteq 5\Gamma \) if \( -1 \in \Gamma \) and \( |\Gamma| \gg \sqrt{p} \log^{1/3} p \).

Let us say a few words about the proof. In [8] O. Roche–Newton obtained that for any set \( A \) from \( \mathbb{R} \) there are \( a, b \in A \) such that

\[
|(A + a)(A + b)| \gg \frac{|A|^2}{\log |A|}.
\]

\*

*This work was supported by grant Russian Scientific Foundation RSF 14–11–00433.*
More precisely, it was proved in [8] that the common multiplicative energy (see the definition in the next section 2) of $A + a$ and $A + b$ is small

$$E^\times(A + a, A + b) \ll |A|^2 \log |A|.$$  \hfill (2)

The proof used the Szemerédi–Trotter theorem from the incidence geometry. Roche–Newton calculated the number of collinear triples in the Cartesian product $A \times A$ in two different ways and comparing the estimates gives (2). In our arguments we use Stepanov’s method [14] in form of Mit’kin [7] (see also [5] and [6]) which allows us to get (1), (2) for $A$ be any multiplicative subgroup of size less than $\sqrt{p}$. It is easy to see that such an analog of (1) implies Theorem 1.

Note also that in the case of multiplicative subgroup $A$ bound (2) is equivalent to

$$E^\times(A + 1) \ll |A|^2 \log |A|$$

because of $A + a = a(A + 1)$, $A + b = b(A + 1)$, $a, b \in A$. Thus, the method allows us to obtain a good upper bound for the multiplicative energy of $A + 1$ (and actually of any shift $A + x$, $x \in \mathbb{F}_p^*$ see Theorem 3 of section 4).

2 Notation

Let $f, g : \mathbb{F}_p \to \mathbb{C}$ be two functions. Put

$$(f * g)(x) := \sum_{y \in \mathbb{F}_p} f(y)g(x - y) \quad \text{and} \quad (f \circ g)(x) := \sum_{y \in \mathbb{F}_p} f(y)g(y + x) \quad (3)$$

Replacing $+$ by the multiplication, one can define the multiplicative convolution of two functions $f$ and $g$. Write $E^+(A, B)$ for the additive energy of two sets $A, B \subseteq \mathbb{F}_p$ (see e.g. [15]), 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,

$$E^+(A, B) = \sum_x (A * B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x)(B \circ B)(x). \quad (4)$$

By $|S|$ denote the cardinality of a set $S \subseteq \mathbb{F}_p$. Note that

$$E^+(A, B) \leq \min\{|A|^2|B|, |B|^2|A|, |A|^{3/2}|B|^{3/2}\}.$$ 

In the same way define the multiplicative energy of two sets $A, B \subseteq \mathbb{F}_p$

$$E^\times(A, B) = |\{a_1b_1 = a_2b_2 : a_1, a_2 \in A, b_1, b_2 \in B\}|.$$

Certainly, multiplicative energy $E^\times(A, B)$ can be expressed in terms of multiplicative convolutions, similar to (4).

Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup. A set $Q \subseteq \mathbb{F}_p^*$ is called $\Gamma$–invariant if $Q\Gamma = Q$. All logarithms are base 2. Signs $\ll$ and $\gg$ are the usual Vinogradov’s symbols.

Notation

Let $f, g : \mathbb{F}_p \to \mathbb{C}$ be two functions. Put

$$(f * g)(x) := \sum_{y \in \mathbb{F}_p} f(y)g(x - y) \quad \text{and} \quad (f \circ g)(x) := \sum_{y \in \mathbb{F}_p} f(y)g(y + x) \quad (3)$$

Replacing $+$ by the multiplication, one can define the multiplicative convolution of two functions $f$ and $g$. Write $E^+(A, B)$ for the additive energy of two sets $A, B \subseteq \mathbb{F}_p$ (see e.g. [15]), 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,

$$E^+(A, B) = \sum_x (A * B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x)(B \circ B)(x). \quad (4)$$

By $|S|$ denote the cardinality of a set $S \subseteq \mathbb{F}_p$. Note that

$$E^+(A, B) \leq \min\{|A|^2|B|, |B|^2|A|, |A|^{3/2}|B|^{3/2}\}.$$ 

In the same way define the multiplicative energy of two sets $A, B \subseteq \mathbb{F}_p$

$$E^\times(A, B) = |\{a_1b_1 = a_2b_2 : a_1, a_2 \in A, b_1, b_2 \in B\}|.$$

Certainly, multiplicative energy $E^\times(A, B)$ can be expressed in terms of multiplicative convolutions, similar to (4).

Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup. A set $Q \subseteq \mathbb{F}_p^*$ is called $\Gamma$–invariant if $Q\Gamma = Q$. All logarithms are base 2. Signs $\ll$ and $\gg$ are the usual Vinogradov’s symbols.
3 On sumsets of multiplicative subgroups

In the section we have deal with the quantity \( T \) for *collinear triples* \( T(A, B, C, D) := \sum_{c \in C, d \in D} E^\times(A - c, B - d) \).

Because \( E^\times(A - c, B - d) \geq |A||B| \) it follows that \( T(A, B, C, D) \geq |A||B||C||D| \). It turns out that there is the same upper bound for \( T \) up to logarithmic factors in the case of \( A, B, C, D \) equal some cosets of a multiplicative subgroup. The proof based on the following lemma of Mit’kin [7], see also [12].

**Lemma 2** Let \( p > 2 \) be a prime number, \( \Gamma, \Pi \) be subgroups of \( \mathbb{F}_p^\times \), \( M_\Gamma, M_\Pi \) be sets of distinct coset representatives of \( \Gamma \) and \( \Pi \), respectively. For an arbitrary set \( \Theta \subset M_\Gamma \times M_\Pi \) such that \( (|\Gamma||\Pi|)^2|\Theta| < p^3 \) and \( |\Theta| \leq 33^{-3}|\Gamma||\Pi| \), we have

\[
\sum_{(u,v) \in \Theta} \left| \{(x, y) \in \Gamma \times \Pi : ux + vy = 1\} \right| \ll (|\Gamma||\Pi|)^{1/3}. \tag{5}
\]

Using the above lemma, we prove the main technical result of the section. The proof is in spirit of [8].

**Proposition 3** Let \( p \) be a prime number, \( \Gamma, \Pi \) be subgroups of \( \mathbb{F}_p^\times \). Suppose that \( |\Gamma||\Pi| < p \). Then

\[
\sum_{\gamma \in \Gamma, \pi \in \Pi} E^\times(\Gamma - \gamma, \Pi - \pi) \ll |\Gamma|^2|\Pi|^2 \log(\min\{|\Gamma|, |\Pi|\}) + |\Gamma||\Pi|( |\Gamma|^2 + |\Pi|^2 ). \tag{6}
\]

**Proof.** Consider the equation

\[
(a - b)(a' - c') = (a - c)(a' - b'), \quad a, b, c \in \Gamma, \quad a', b', c' \in \Pi. \tag{7}
\]

Clearly, the number of its solutions is

\[
T(\Gamma, \Pi, \Gamma, \Pi) = \sum_{\gamma \in \Gamma, \pi \in \Pi} E^\times(\Gamma - \gamma, \Pi - \pi). \]

One can assume that the products in (7) are nonzero and \( b \neq c \) because otherwise we have at most \( O(|\Gamma|^3|\Pi| + |\Gamma||\Pi|^3 + |\Pi|^2|\Gamma|^2) \) number of the solutions. Denote by \( \sigma \) the remaining number of the solutions.

Take a parameter \( \tau \geq 2 \) and put

\[
\Theta_\tau := \{(u, v) \in M_\Gamma \times M_\Pi : |\{(x, y) \in \Gamma \times \Pi : ux + vy = 1\}| \geq \tau\}. \]

In other words, \( \Theta_\tau \) counts the number of lines \( l_{u,v} = \{(x, y) : ux + vy = 1\}, (u, v) \in M_\Gamma \times M_\Pi \) having the intersection with \( \Gamma \times \Pi \) greater than \( \tau \). Obviously, if \( (u, v) \equiv (u', v') \mod (\Gamma \times \Pi) \),
then the intersections of lines \( l_{u,v} \) and \( l_{u',v'} \) with \( \Gamma \times \Pi \) are coincide. By Lemma 2 we have \( |\Theta_\tau| \ll |\Gamma||\Pi|^{r-3} \) provided \((|\Gamma||\Pi|)^2 |\Theta_\tau| < p^3 \) and \( |\Theta_\tau| \leq 33^{-3}|\Gamma||\Pi| \). Thus

\[
q_\tau := \{(u, v) : |\{(x, y) \in \Gamma \times \Pi : ux + vy = 1\}| \geq \tau \} \ll |\Gamma|^2|\Pi|^2|\tau|^{-3}
\]

provided \((|\Gamma||\Pi|)^2 |\Theta_\tau| < p^3 \) and \( |\Theta_\tau| \leq 33^{-3}|\Gamma||\Pi| \). The number of all lines intersecting \( \Gamma \times \Pi \) by at least two points does not exceed \( |\Gamma|^2|\Pi|^2 \). Thus, splitting \( \Theta_\tau \) onto smaller sets if its required, we get upper bound (8) for \( q_\tau \) with possibly bigger absolute constant, provided the only condition \((|\Gamma||\Pi|)^2 |\Theta_\tau| < p^3 \) holds. The assumption \( |\Gamma||\Pi| < p \) implies the last inequality.

It is easy to see that for any tuple \((a, a', b, b', c, c')\) satisfying (7), the points \((a, a'), (b, b'), (c, c')\) lies at the same line and these points are pairwise distinct. Clearly, the number of such triples belonging the lines having the form \( ux + vy = 0 \) and intersecting \( \Gamma \times \Pi \) does not exceed \((|\Gamma||\Pi|)^2\), so it is negligible. Thus, using (8), we see that the rest of the quantity \( \sigma \) is less than

\[
\sum_{u,v} |l_{u,v} \cap (\Gamma \times \Pi)|^2 \ll \sum_{j \geq 1} \sum_{u,v : 2^{j-1} < |l_{u,v} \cap (\Gamma \times \Pi)| \leq 2^j} |l_{u,v} \cap (\Gamma \times \Pi)|^3 \ll \sum_{j \geq 1} 2^{3j} \cdot |\Gamma|^2|\Pi|^2 \cdot 2^{-3j} \ll |\Gamma|^2|\Pi|^2 \log(\min\{|\Gamma|, |\Pi|\}).
\]

This completes the proof. \( \square \)

**Remark 4** Careful analysis of the proof gives that one can assume that \( a, b, c \) belong to different cosets of \( \Gamma \) and \( a', b', c' \) are from different cosets of \( \Pi \) (it will be three Cartesian products of cosets instead of one in the case). In particular, the following holds

\[
\sum_{\gamma \in \xi \Gamma, \pi \in \eta \Pi} E^\times (\Gamma - \gamma, \Pi - \pi) \ll |\Gamma|^2|\Pi|^2 \log(\min\{|\Gamma|, |\Pi|\}) + |\Gamma||\Pi|(|\Gamma|^2 + |\Pi|^2),
\]

where \( \xi, \eta \in \mathbb{F}_p^* \) are arbitrary. Of course, one can permute \( \Gamma \) to \( \xi \Gamma \) and \( \Pi \) to \( \eta \Pi \) in formula (9).

Proposition 3 allows us to prove new results on sumsets of subgroups, which improve some bounds from [2], see Lemma 7.3 and also Lemma 7.4.

**Corollary 5** Let \( p \) be a prime number, \( \Gamma \subset \mathbb{F}_p^* \) be a multiplicative subgroup, \( |\Gamma| < \sqrt{p} \). Then

\[
\left| \left\{ \frac{a \pm b}{a \pm c} : a, b, c \in \Gamma \right\} \right| \gg \frac{|\Gamma|^2}{\log |\Gamma|},
\]

and for any \( X \subseteq \Gamma \) one has

\[
|2\Gamma + X| \gg \frac{|X|^2}{\log |\Gamma|}.
\]

In particular

\[
|3\Gamma| \gg \frac{|\Gamma|^2}{\log |\Gamma|}.
\]
Proof. The first estimate follows from the Cauchy–Schwarz inequality and the interpretation of the quantity 
\[ T(\Gamma, \Pi, \Gamma, \Pi) \] as the number of the solutions of (7). To get the second estimate apply (9) with \( \Gamma = \Gamma, \Pi = \Gamma, \xi = \eta = -1 \). We find \( \gamma_1, \gamma_2 \in \Gamma \) such that
\[ E^{\times}((\Gamma + \gamma_1, \Gamma + \gamma_2) \ll |\Gamma|^2 \log |\Gamma|. \]

By the Cauchy–Schwarz inequality, we get
\[ |(\Gamma + \gamma_1)\cdot (X + \gamma_2)| \cdot E^{\times}(\Gamma + \gamma_1, \Gamma + \gamma_2) \geq |(\Gamma + \gamma_1)\cdot (X + \gamma_2)| \cdot E^{\times}(\Gamma + \gamma_1, X + \gamma_2) \geq |\Gamma|^2 |X|^2. \]

Note that \( (\Gamma + \gamma_1)(X + \gamma_2) \subseteq 2\Gamma + \gamma_1X + \gamma_1\gamma_2 \). Moreover, \( |2\Gamma + \gamma_1X + \gamma_1\gamma_2| = |2\Gamma + X| \). Hence
\[ |2\Gamma + X| \geq |(\Gamma + \gamma_1)(X + \gamma_2)| \gg \frac{|X|^2}{\log |\Gamma|} \]
as required.

We are going to apply the method of the section to the problems concerning decompositions of multiplicative subgroups in the future paper.

4 Generalizations

First of all, we derive a consequence of Proposition\ref{thm:generalization} concerning multiplicative energies of shifts of subgroups.

**Theorem 6** Let \( p \) be a prime number, \( \Gamma, \Pi \) be multiplicative subgroups of \( \mathbb{F}_p^* \). Suppose that \( |\Gamma||\Pi| < p \). Then for any \( x, y \neq 0 \) one has
\[ E^{\times}(\Gamma + x, \Pi + y) \ll |\Gamma||\Pi|\log(\min\{|\Gamma|, |\Pi|\}) + |\Gamma|^2 + |\Pi|^2. \]

Proof. Since \( x, y \neq 0 \) it follows that \( x \in \xi\Gamma, y \in \eta\Pi \) and \( \xi, \eta \neq 0 \). Further, it is easy to see that
\[ E^{\times}(\Gamma + x, \Pi + y) = E^{\times}(\xi^{-1}\Gamma + \gamma, \eta^{-1}\Pi + \pi) \]
for any \( \gamma \in \Gamma \) and \( \pi \in \Pi \). Thus, all energies in the left–hand side of formula \ref{thm:generalization} are coincide. This completes the proof.

It is interesting to compare the last theorem with results of \cite{Konyagin} and \cite{Konyagin2} which give a pointwise bound for the multiplicative convolution of characteristic functions of multiplicative subgroups in contrary to our average estimate.

Using a formula
\[ E^+(\Gamma) = E^{\times}(\Gamma, \Gamma + 1) \]
for an arbitrary subgroup \( \Gamma \), we derive by the Cauchy–Schwarz inequality and Theorem\ref{thm:generalization} that
\[ E^+(\Gamma) \ll |\Gamma|^{5/2} \log^{1/2} |\Gamma|. \] This coincides with Konyagin’s bound \cite{Konyagin} up to logarithmic factors.

Let us prove a generalization of Proposition\ref{thm:generalization} and Theorem\ref{thm:generalization}.
Theorem 7 Let \( p \) be a prime number, \( \Gamma, \Pi \) be multiplicative subgroups of \( \mathbb{F}_p^* \). Suppose that \( |\Gamma||\Pi| < p \) and \( Q_1 \) is \( \Gamma \)-invariant, \( Q_2 \) is \( \Pi \)-invariant sets. Then
\[
T(Q_1, Q_2, Q_1, Q_2) \ll (|Q_1||Q_2|)^3(|\Gamma||\Pi|)^{-1} \log^2(\min\{|Q_1|, |Q_2|\}) + |Q_1||Q_2|(|Q_1|^2 + |Q_2|^2). \tag{10}
\]

Proof. Let \( L = \log(\min\{|Q_1|, |Q_2|\}) \). We use the arguments of Proposition \( \text{[3]} \). The term \( |Q_1||Q_2|(|Q_1|^2 + |Q_2|^2) \) appears similarly as in the proof and thus we are considering the set of lines (pairs)
\[
\mathcal{L}_\tau := \{(u, v) : |\{(x, y) \in Q_1 \times Q_2 : ux + vy = 1\}| \geq \tau\}
\]
intersecting \( Q_1 \times Q_2 \) in at least three distinct points. Let \( Q_1 \times Q_2 = \bigcup_{i=1}^{s} C_i \), where \( C_i \) are products of the correspondent cosets, \( s = |Q_1||Q_2||\Gamma|^{-1}|\Pi|^{-1} \). Taking a line \( l \in \mathcal{L}_\tau \) and using the Dirichlet principle, we find a number \( \Delta(l) \) such that
\[
\tau \leq |l \cap (Q_1 \times Q_2)| \leq \sum_{i=1}^{s} |l \cap C_i| \ll L \Delta(l) |\Omega_\Delta(l)|,
\]
where
\[
\Omega_\Delta(l) = \{i : \Delta < |l \cap C_i| \leq 2\Delta\},
\]
and \( \Delta(l) \geq \max\{\tau s^{-1}, 1\} \). The number \( \Delta(l) \) depends on \( l \) but using the Dirichlet principle again, we find a set \( \mathcal{L}'_\tau \subseteq \mathcal{L}_\tau, |\mathcal{L}'_\tau| \gg |\mathcal{L}_\tau| L^{-1} \) with some fixed \( \Delta \geq \max\{\tau s^{-1}, 1\} \). After that, using the arguments of Proposition \( \text{[3]} \) we see that
\[
|\mathcal{L}_\tau| L^{-1} \ll |\mathcal{L}'_\tau| \ll \frac{|\Gamma|^2 |\Pi|^2}{\Delta^3} \ll \frac{|\Gamma|^2 |\Pi|^2 s^3}{\tau^3}
\]
and we have obtained \( \text{[10]} \).

Let us give another proof. Take the same family of the lines \( \mathcal{L}'_\tau \) and consider a smaller family of points \( \mathcal{P}' := \bigcup_{l \in \mathcal{L}'_\tau} \bigcup_{i \in \Omega_\Delta(l)} C_i \). Using Lemma \( \text{[2]} \) as well as the arguments of the proof of Proposition \( \text{[3]} \) again, we see that any line meets at most \( |\Gamma||\Pi|\Delta^{-3} \) cells \( C_i \). In other words, \( |\Omega_\Delta(l)| \ll |\Gamma||\Pi|\Delta^{-3} \). Let us calculate the number of indices \( I(\mathcal{L}'_\tau, \mathcal{P}') \) between lines from \( \mathcal{L}'_\tau \) and points \( \mathcal{P}' \). On the one hand, any line from \( \mathcal{L}'_\tau \) contains at least \( \Delta |\Omega_\Delta(l)| \gg \tau L^{-1} \) number of points. Thus,
\[
I(\mathcal{L}'_\tau, \mathcal{P}') \gg \Delta |\mathcal{L}'_\tau| |\Omega_\Delta(l)| \gg |\mathcal{L}'_\tau| \tau L^{-1}.
\]
On the other hand, by a trivial estimate for the number of indices between points and lines (see e.g. \( \text{[15]}, \text{section 8.2} \)), we get
\[
I(\mathcal{L}'_\tau, \mathcal{P}') \leq \sum_{i=1}^{s} I(\mathcal{L}'_\tau, \mathcal{P}' \cap C_i) \leq \sum_{i=1}^{s} \left( |\mathcal{P}' \cap C_i| |L_i|^{1/2} + |L_i| \right),
\]
where by \( L_i \) we denote the lines from \( \mathcal{L}'_\tau \), intersecting \( C_i \). Clearly, \( |\mathcal{P}' \cap C_i| = |\Gamma||\Pi| \). Further, because of any line \( l \) meets at most \( |\Omega_\Delta(l)| \ll |\Gamma||\Pi|\Delta^{-3} \) cells \( C_i \), we see that
\[
\sum_{i=1}^{s} |L_i| \ll |\mathcal{L}'_\tau| \cdot |\Gamma||\Pi|\Delta^{-3}.
\]
Using the estimate $|\Omega_\Delta(l)| \Delta \gg \tau L^{-1}$, the Cauchy–Schwarz inequality and the lower bound for $I(L', \mathcal{P})$, we obtain

$$|L|^{-1} \ll |L'| \ll \frac{L|\Gamma|^2|\Pi|^2 s}{\Delta \tau} \ll \frac{L|\Gamma|^2|\Pi|^2 s}{\tau \max\{1, \tau s^{-1}\}}.$$ 

After some calculations we have (10). This completes the proof. □

**Corollary 8** Let $p$ be a prime number, $\Gamma$ be a multiplicative subgroup of $\mathbb{F}_p^*$, $|\Gamma| < \sqrt{p}$, and $Q$ be $\Gamma$–invariant set. Then there is $q \in Q$ such that

$$E^x(Q - q, \Gamma + x) \ll |Q|^2 \log^2 |\Gamma|,$$

where $x \in \mathbb{F}_p^*$ is an arbitrary.

**Remark 9** Considering $T(Q_1, Q_2, \xi Q_1, \eta Q_2)$, where $\xi \neq 0, 1$ or $\eta \neq 0, 1$ one can reduce the term $|Q_1||Q_2|(|Q_1|^2 + |Q_2|^2)$ in formula (10) of Theorem 7 sometimes. For example, if $\Gamma$ is a subgroup, $Q$ is $\Gamma$–invariant set then the correspondent error term in $T(\Gamma, Q, \xi \Gamma, Q)$, $\xi \neq 0, 1$ is $O(|\Gamma|^3|Q| + |\Gamma|^2|Q|^2)$, thus it is negligible.

**References**

[1] T. Cochrain, C. Pinner, *Sum–product estimates applied to Waring’s problem mod p*, Integers 8 (2008), A46, 1–18.

[2] T. Cochrain, D. Hart, C. Pinner, C. Spencer, *Waring’s number for large subgroups of double–struck $\mathbb{Z}_p$*, Acta Arithmetica, 163:4 (2014), 309–325.

[3] A. A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erdöš-Graham problem*, Mat. Zametki, 79 (2006), 384–395; translation in: Math. Notes 79 (2006), 356–365.

[4] D. Hart, *A note on sunsets of subgroups in $\mathbb{Z}_p^*$*, [arXiv:1303.2729v2 [math.CO]] 23 May 2013.

[5] S. V. Konyagin, *Estimates for trigonometric sums and for Gaussian sums*, IV International conference "Modern problems of number theory and its applications". Part 3 (2002), 86–114.

[6] S. V. Konyagin, I. Shparlinski, *Character sums with exponential functions*, Cambridge University Press, Cambridge, 1999.

[7] D. A. Mit’kin, *Estimation of the total number of the rational points on a set of curves in a simple finite field*, Chebyshevsky sbornik, 4:4(2003), 94–102.

[8] O. Roche–Newton, *A short proof of a near–optimal cardinality estimate for the product of a sum set*, [arXiv:1502.05560v1 [math.CO]] 19 Feb 2015.
[9] T. Schoen, I. D. Shkredov, Additive properties of multiplicative subgroups of $\mathbb{F}_p$, Quart. J. Math. 63:3 (2012), 713–722.

[10] I.D. Shkredov, Some new inequalities in additive combinatorics, Moscow J. Combin. Number Theory 3 (2013), 237–288.

[11] I.D. Shkredov, On exponential sums over multiplicative subgroups of medium size, Finite Fields and Their Applications 30 (2014), 72–87.

[12] I. Shkredov, E. Solodkova, I. Vyugin, Intersections of multiplicative subgroups and Heilbronn’s exponential sum, arXiv:1302.3839v2 [math.NT] 1 Aug 2014.

[13] I. D. Shkredov, I. V. Vyugin, On additive shifts of multiplicative subgroups, Mat. Sbornik 203:6 (2012), 81–100.

[14] S. A. Stepanov, On the number of points on hyperelliptic curve over prime finite field, IAN 33 (1969), 1171–1181.

[15] T. Tao and V. Vu, Additive Combinatorics, Cambridge University Press (2006).

[16] P. Corvaja, U. Zannier, Greatest common divisors of $u - 1$, $v - 1$ in positive characteristic and rational points on curves over finite fields, J. Eur. Math. Soc. 15 (2013), 1927–1942.

[17] I. Vyugin, S. Makarichev, On the number of solutions of polynomial equation over $\mathbb{F}_p$, arXiv:1504.01354v1 [math.NT] 26 Mar 2015.

I.D. Shkredov
Steklov Mathematical Institute,
ul. Gubkina, 8, Moscow, Russia, 119991

and

IITP RAS,
Bolshoy Karetny per. 19, Moscow, Russia, 127994

ilya.shkredov@gmail.com