ЧЕБЫШЕВСКИЙ СБОРНИК
Том 18 Выпуск 2

УДК 511.321 DOI 10.22405/2226-8383-2017-18-2-267-274

СУММЫ ХАРАКТЕРОВ НА СДВИНУТЫХ СТЕПЕНЯХ

Ю.Н. Штейников (г. Москва)

Аннотация

Мы изучаем суммы характеров на множестве сдвинутых степеней по модулю простого числа p. Такие суммы могут рассматриваться как обобщение сумм характеров от сдвинутой подгруппы. Случай, когда подгруппа имеет размер меньше $\sqrt{p}$, вопрос о нетривиальных по порядку верхних оценок таких сумм остается открытым и на сегодня является нерешенным. Он был предложен Ж. Бургейном и М.Ч. Чанг в обзоре 2010 года. Тем не менее, некоторых промежуточных результатов добился профессор К. Гонг, установивший нетривиальные оценки таких сумм в случае когда подгруппа имеет размер существенно больше $\sqrt{p}$. В данной работе получены некоторые новые результаты на верхнюю оценку абсолютного значения обобщения таких сумм, которые являются неполными суммами характеров от сдвинутых подгрупп. Дано два доказательства основного утверждения. Первое из них основано на сведении указанной суммы к известной оценке А. Вейля и приеме сглаживания сумм. Применяется также прием оценки неполной суммы через полную. Используется также один результат М.З. Гараева. Второе доказательство основано на оригинальной идее И.М. Виноградова. Этот подход был предложен для уточнения известного неравенства Пойа-Виноградова и использует в своей сути некоторые геометрические и комбинаторные идеи. Второе доказательство приведено не в полной мере. Мы лишь доказываем некоторое ключевое утверждение и за остальными выкладками отсылаем читателя к самой работе И.М. Виноградова.

Ключевые слова: конечные поле, степени, суммы.

Библиография: 15 названий.

CHARACTER SUMS OVER SHIFTED POWERS

Yu.N. Shteinikov (Moscow)

Abstract

We study character sums over shifted powers modulo a prime p. Such sums can be viewed as generalizations of character sums over shifted multiplicative subgroups. We obtain some new results on upper estimates for absolute value of these sums. The case when the cardinality of subgroup is less than $\sqrt{p}$, it is a question of non-trivial upper bounds for such sums that remains open and is unsolved today. It was proposed by J. Burgain and M.Ch. Chang in the review of 2010. Nevertheless, some intermediate results were achieved by Professor K. Gong, who established non-trivial estimates of such sums in the case when the subgroup is much larger than $\sqrt{p}$. In this paper, we obtain some new results on the upper bound for the absolute value of the generalization of such sums, which are incomplete sums of character sums over shifted subgroups. Two proofs of the main result are given. The first one is based on reduction of this sum to the well-known estimate of A. Weil and the method of smoothing such sums. The method of estimating the incomplete sum through the full one is also applied. One result of M.Z. Garaev is also used. The second proof is based on the original idea of I.M. Vinogradov. This approach was proposed to refine the known inequality of Poya-Vinogradov and uses in its

essence some geometric and combinatorial ideas. The second proof is not fully presented. We only prove a key statement, and for the rest of the calculations we refer the reader to the initial work of I.M. Vinogradov.

Keywords: finite field, powers, sums.

Bibliography: 15 titles.

1. Introduction

Throughout the paper n - is positive integer and $p-$ is an odd large prime number, $\mathbb{Z}_n$ be the $n-$ element residue ring and $\mathbb{Z}_n^*-$ multiplicative group of $\mathbb{Z}_n$. Let χ is some multiplicative character modulo n, $\gcd(a,n)=1$, and $l \in \mathbb{Z}_n^*$, with $ord(l)=L$, that means L is the minimal positive integer n that $l^n \equiv 1 \pmod n$. For $1 \le K \le L$

denote

$$S(\chi,a,l,K) := \sum_{1\le k\le K} \chi(a+l^k), \qquad (a,n)=1.$$

Hong Bing Yu obtained [1] non-trivial upper estimates for $S(\chi,a,l,K)$. We formulate his result below.

Теорема 1. *Let $n \ge 2$ and $\chi-$ is a primitive Dirichlet character modulo n. The following estimate holds*

$$|S(\chi,a,l,K)| < \sqrt{n}(\frac{2}{\pi}\log n + \frac{7}{5}).$$

Let $G \subset \mathbb{Z}_n^*-$ multiplicative subgroup and

$$S(\chi,a,G) := \sum_{x\in G} \chi(a+x).$$

It is an opened question to obtain nontrivial upper estimates for $|S(\chi,a,G)|$ when $G \subset \mathbb{Z}_p^*$ and $G \sim p^{\frac{1}{2}}$. Jean Bourgain posed this problem (see M.-C. Chang's 2010 survey). The exact formulation of it is the following.

Problem (J. Bourgain) Let G - subgroup, $G \subset \mathbb{Z}_p^*$, $|G| \sim p^{\frac{1}{2}}, p \to \infty$, χ – nontrivial character modulo p, $\gcd(a,p)=1$. Obtain nontrivial upper estimate in the following form

$$|S(\chi,a,G)| = o(|G|), p \to \infty.$$

In this paper we consider upper esimates for $|S(\chi,a,l,K)|$ in the case of prime modulo p. (χ – is a multiplicative character modulo p.)

The main aim of this paper is to give a nontrivial bound for absolute value of $S(\chi,a,l,K)$ when K is sufficiently large than $p^{\frac{1}{2}}$. The main result is contained in the following theorem.

Теорема 2. *Let $K \ge p^{\frac{1}{2}}$, $\chi-$ is a multiplicative character modulo p. Than the following estimate holds*

$$|S(\chi,a,l,K)| \ll \sqrt{p}(\log\frac{K}{\sqrt{p}} + 1).$$

In the case of prime modulo the quantities $S(\chi,a,l,K)$ can be considered as generalizations of $S(\chi,a,G)$. Indeed, any subgroup $G \subset \mathbb{Z}_p^*$ is cyclic, that means $G = \{l^k\}_{1\le k\le |G|}$ for some $l \in \mathbb{Z}_p^*$. Estimates of character sums for different variants were considered in numerous papers, let us note the works [6], [3], [9],[10], [11],[12], [7], [8].

We recall that the notations $A(n) = O(B(n)), A(n) \ll B(n)$ are equivalent to the statement that there exists an absolute constant c that inequality $|A(n)| \le cB(n)$ holds for all n.

2. Preliminary results

In this section we collect some facts and lemmas which we will use in the proof of main results. But we shall start with upper estimates for $|S(\chi, a, G)|$ which were obtained by Ke Gong.

Proposition 1. *Let $G \subset \mathbb{Z}_p^*$ –is any multiplicative subgroup, than we have*

$$|S(\chi, a, G)| \le p^{1/2}.$$

In the proof we use I. M. Vinogradov's lemma, (see it in [13]) which is given below.

Lemma 1. *Let*

$$S := \sum_{0\le x\le p-1} \sum_{0\le y\le p-1} \alpha(x)\beta(y)\chi(xy+a),$$

with

$$\sum_{0\le x\le p-1} |\alpha(x)|^2 \le X, \sum_{0\le y\le p-1} |\alpha(y)|^2 \le Y$$

Then we have

$$|S| \le (pXY)^{\frac{1}{2}}.$$

Now we are ready to prove proposition 3.

Доказательство. Let $G(x)$– be the indicator of G. We have

$$\sum_{x\in G} \chi(x+a) = \frac{1}{|G|} \sum_{x,y\in G} \chi(xy+a) = \frac{1}{|G|} \sum_{0\le x\le p-1} \sum_{0\le y\le p-1} G(x)G(y)\chi(xy+a).$$

Applying Vinogradov's lemma to the last sum we obtain the desired estimate. Thus, proposition 3 is proved. □

Let function $f\colon \mathbb{Z}_L \to \mathbb{C}$. We recall tha Fourier transform $\hat{f}(\xi)$ is defined as

$$\hat{f}(\xi) := \frac{1}{L} \sum_{x=1}^{L} f(x) e^{-2\pi i \frac{\xi x}{L}},$$

and

$$f(x) = \sum_{\xi=1}^{L} \hat{f}(\xi) e^{2\pi i \frac{\xi x}{L}}.$$

We will use the well known Weil estimate of character sums.

Lemma 2. *Let χ– is a multiplicative character of $\mathbb{Z}_p^*$ of order $m > 1$ and $f \in \mathbb{Z}_p[x]$ - is a polynomial with positive degree and with d distinct zeros in $\overline{\mathbb{Z}_p}$ and which is not a m–th power of another polynomial. Then we have following estimate*

$$|\sum_{x\in\mathbb{Z}_p} \chi(f(x))| \le dp^{\frac{1}{2}}.$$

The next result belongs to M. Garaev[2] and we will use it.

Lemma 3. *Let L_1, L_2, A, B and L be any integers, $1 \le A, B \le L$. Then*

$$W := \sum_{a=0}^{L-1} \Big| \sum_{x=L_1+1}^{L_1+A} e^{2\pi i a x/L} \Big| \Big| \sum_{y=L_2+1}^{L_2+B} e^{2\pi i a y/L} \Big| \ll LA\log(BA^{-1}+2)$$

Let us denote

$$f(k) := \chi(a + l^k).$$

In the next lemma we get estimates on $\hat{f}(\xi)$.

Lemma 4. *For any ξ the following estimate holds*

$$|\hat{f}(\xi)| \le \frac{\sqrt{p}}{L}.$$

Доказательство. We have $\hat{f}(\xi) = \frac{1}{L}\sum_{k=1}^{L} \chi(a+l^k)e^{-2\pi i\frac{\xi k}{L}}$. Let $d := \frac{p-1}{L}$. For some primitive root g modulo p we have $l = g^d$, and we have

$$\hat{f}(\xi) = \frac{1}{p-1}\sum_{k=1}^{p-1} \chi(a + g^{dk})e^{-2\pi i\frac{\xi k}{L}}.$$

Denoting $x = g^k$ and so $k = ind_g x$, we get

$$\hat{f}(\xi) = \frac{1}{p-1}\sum_{x=1}^{p-1} \chi(a + x^d)e^{-2\pi i\frac{\xi (ind_g x)}{L}}.$$

We see that the function $e^{-2\pi i\frac{\xi (ind_g x)}{L}}$ as the function of x is some multiplicative character $\chi_\xi(x)$. Therefore

$$\hat{f}(\xi) = \frac{1}{p-1}\sum_{x=1}^{p-1} \chi(a + x^d)\chi_\xi(x).$$

Each of the characters χ, χ_ξ is a power of some fixed multiplicative character χ_1,

$$\chi = \chi_1^{m_1}, \chi_\xi = \chi_1^{m_2}.$$

so

$$\hat{f}(\xi) = \frac{1}{p-1}\sum_{x=1}^{p-1} \chi_1((a + x^d)^{m_1}x^{m_2}).$$

Next, we use Weil estimate, – lemma 5 and get the desired estimate. With that we finish the proof. □

3. The proof of the main results.

Доказательство. For the proof of theorem 2 we need to estimate $|\sum_{n=A+1}^{A+K} f(n)|$, and we can assume that $\sqrt{p} < K < p^{0.99}$. Let us denote

$$g(n) := \sum_{k=n}^{n+[\sqrt{p}]-1} f(k).$$

Consider the following sum

$$\sigma := \sum_{n=A-[\sqrt{p}]+2}^{A+K} g(n).$$

It is easy to see that

$$\sigma = [\sqrt{p}](\sum_{n=A+1}^{A+K} f(n)) + O(p).$$

So we will get upper estimate for $|\sigma|$.

We define $I := [A - [\sqrt{p}] + 2, A + K]$. We have

$$\sigma = \sum_{k\in I} g(k) = \sum_{k=0}^{L-1} g(k) \sum_{k'\in I} \frac{1}{L} \sum_{a=0}^{L-1} e^{2\pi i \frac{a(k'-k)}{L}} = \frac{1}{L} \sum_{a=0}^{L-1} (\sum_{k=0}^{L-1} g(k) e^{2\pi i \frac{-ak}{L}})(\sum_{k'\in I} e^{2\pi i \frac{ak'}{L}}) =$$

$$= \sum_{a=0}^{L-1} \hat{g}(a) \sum_{k'\in I} e^{2\pi i \frac{ak'}{L}}$$

For $\hat{g(a)}$ we have –

$$\hat{g}(a) = \frac{1}{L} \sum_{x=0}^{L-1} \sum_{k=0}^{[\sqrt{p}]-1} f(x+k) e^{-2\pi i \frac{ax}{L}} = \frac{1}{L} \sum_{x=0}^{L-1} f(x) (\sum_{k=0}^{[\sqrt{p}]-1} e^{-2\pi i \frac{a(x-k)}{L}}) =$$

$$= \hat{f}(a) \sum_{k=0}^{[\sqrt{p}]-1} e^{2\pi i \frac{ak}{L}}.$$

So, inserting this to the expression for σ we obtain

$$\sigma := \sum_{a=0}^{L-1} \hat{f}(a) \sum_{k''=0}^{[\sqrt{p}]-1} e^{2\pi i \frac{ak''}{L}} \sum_{k'\in I} e^{2\pi i \frac{ak'}{L}}.$$

Recalling estimates for $|\hat{f}(a)|$ in lemma 7

$$|\sigma| \le \frac{[\sqrt{p}]}{L} \sum_{a=0}^{L-1} |\sum_{k''=0}^{[\sqrt{p}]-1} e^{2\pi i \frac{ak''}{L}}| |\sum_{k'\in I} e^{2\pi i \frac{ak'}{L}}|.$$

Using lemma 6 we easily derive the desired estimate for σ and so for initial sum. With that we finish the proof of theorem 2. □

4. Final Remarks

There is another way to prove theorem 2.

Professor Ke Gong pointed me on it so I include it here.

It can be done using approach of I.M. Vinogradov [10], where he considered upper bounds for $|\sum_{m\le k\le M+q} \chi(k)|$. We are only going give a sketch of this proof. Denoting

$$f(k) := \chi(a + l^k),$$

so we need to obtain upper bound for $|\sum_{1\le k\le K} f(k)|$. Following the proof as in [10], we need to establish the following key lemma.

LEMMA 5. *Let $P, M_1, \dots, M_m \in \mathbb{N}, P < \frac{L}{2}$ and*

$$M_1 + P \le M_2, \dots, M_{m-1} + P \le M_m \le M_1 + L$$

Then we have

$$\sum_{1\le i\le m} \left| \sum_{M_i+1\le x\le M_i+P} \sum_{0\le z\le P-1} f(x+z) \right| \ll (mp)^{\frac{1}{2}} P.$$

Let W is the following set

$$W := \{x \in \mathbb{Z}_p : \exists i \in [1,m], \exists k \in [M_i+1, M_i+P], x \equiv l^k \pmod p\}$$

and $W(x)$ is indicator function of set W. So we have

$$\sum_{1\le i\le m}\left|\sum_{M_i+1\le x\le M_i+P}\sum_{0\le z\le P-1} f(x+z)\right| \ll \sum_{0\le x\le p-1} W(x)\left|\sum_{0\le z\le P-1}\chi(a+xl^z)\right|.$$

Next, we use Cauchy-Shwartz inequality and after we should obtain estimate for

$$\sum_{0\le x\le p-1}\left|\sum_{0\le z\le P-1}\chi(a+xl^z)\right|^2.$$

Taking the square of inner sum and changing the order of summation one can easily get the desired estimate. This is the way of proving lemma 8.

The final arguments for the proof of theorem 2 can be found in [10]. There are some kind of geometrical and approximation argumets in the proof.

Acknowledgements

I want to thank professor Jia Chaohua for invition on the Chinese-Russian workshop on exponential sums and sumsets in Beijing in november 2015, for its hospitality and excellent working conditions. The task of this paper appeared while being on that workshop. I also want to thank professors Ke Gong and Sergei Konyagin for valuable advices.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Hong Bing Yu, *Estimates of character sums with exponential function* // Acta Arithmetica. 2001. Vol. 97, №3, P. 211-218.

2. M. Z. Garaev, *On the logarithmic factor in error term estimates in certain additive congruence problems* // Acta Arith. 2006. Vol 124 , P. 27–39.

3. L. Goldmakher, *Multiplicative mimicry and improvements of the P?lya-Vino gradov inequality*// Algebra and Number Theory 2012. Vol. 6, No. 1, P. 123–163.

4. C. Dartyge and A. Sárközy, *On additive decompositions of the set of primitive roots modulo p*// Monatsh. Math. 2013. Vol 169, P 317–328.

5. K. Gong, C. Jia, M.A. Korolev, Shifted character sums with multiplicative coefficients, II // J. Number Theory, 2017, Vol 178, P.31–39.

6. D.A. Frolenkov *A numerically explicit version of the Polya-Vinogradov inequality* // Moscow journal of Combinatorics and Number Theory, 2011, Vol 1, № 3, P. 25–41.

7. D. A. Frolenkov, K. Soundararajan *A generalization of the Po?lya–Vinogradov inequality* // Ramanujan J., 2013 Vol 31, № 3 , P. 271–279.

8. C. Pomerance *Remarks on the Polya-Vinogradov inequality*// IMRN, 2011, Vol 151, P. 30–41.

9. E. Dobrowolski, K. S. Williams *An upper bound for the sum* $\sum_{n=a+1}^{a+H} f(n)$*for a certain class of funktions* f // Proccedings of the American Mathematical Society, 1992, Vol 114, № 1, P. 29–35.

10. I. M. Vinogradov *A new improvement of the method of estimation of double sums (Russian)*// Doklady Akad. Nauk SSSR (N.S), 1950, Vol 73, P. 635–638.

11. A. Granville, K. Soundararajan *Large character sums: pretentious characters and the Polya-Vinogradov theorem*// J. Amer. Math. Soc. (N.S), 2007, Vol.20, P. 357–384.

12. G. Bachman, L. Rachakonda *On a problem of Dobrowolski and Williams and the Polya-Vinogradov inequality* // Ramanujan J., 2001, Vol 5, P. 65–71.

13. I. M. Vinogradov *Basics of number theory*// Gostechizdat (1952), 1–180.

14. A. A. Karatsuba *Basics of analytic number theory.* URSS (2004), 1–182.

15. T. Tao , V. Vu *Additive combinatorics.* Cambridge University Press 2006, P. 1-530.

REFERENCES

1. Hong Bing Yu, *Estimates of character sums with exponential function* // *Acta Arithmetica* 2001. vol. 97, no. 3, pp. 211-218.

2. M. Z. Garaev, *On the logarithmic factor in error term estimates in certain additive congruence problems Acta Arith* 2006. Vol 124, pp. 27–39.

3. L. Goldmakher, *Multiplicative mimicry and improvements of the P?lya-Vino gradov inequality Algebra and Number Theory* 2012. vol. 6, no. 1, pp. 123–163.

4. C. Dartyge and A. Sárközy, *On additive decompositions of the set of primitive roots modulo p Monatsh. Math.* 2013. vol 169, pp. 317–328.

5. K. Gong, C. Jia, M.A. Korolev, Shifted character sums with multiplicative coefficients, II *J. Number Theory* 2017, vol 178, pp. 31–39.

6. D.A. Frolenkov *A numerically explicit version of the Polya-Vinogradov inequality Moscow journal of Combinatorics and Number Theory* 2011, vol 1, no. 3, pp. 25–41.

7. D. A. Frolenkov, K. Soundararajan *A generalization of the Polya–Vinogradov inequality Ramanujan J.* 2013. vol 31, no 3 , pp. 271–279.

8. C. Pomerance *Remarks on the Polya-Vinogradov inequality IMRN* 2011, vol 151, pp. 30–41.

9. E. Dobrowolski K. S. Williams *An upper bound for the sum* $\sum_{n=a+1}^{a+H} f(n)$*for a certain class of funktions* f *Proccedings of the American Mathematical Society*, 1992, vol 114, no 1, pp. 29–35.

10. I. M. Vinogradov *A new improvement of the method of estimation of double sums (Russian) Doklady Akad. Nauk SSSR (N.S)* 1950, vol 73, pp. 635–638.

11. A. Granville, K. Soundararajan *Large character sums: pretentious characters and the Polya-Vinogradov theorem J. Amer. Math. Soc. (N.S)* 2007, vol.20, pp. 357–384.

12. G. Bachman, L. Rachakonda *On a problem of Dobrowolski and Williams and the Polya-Vinogradov inequality Ramanujan J.* 2001, vol 5, pp. 65–71.

13. I. M. Vinogradov *Basics of number theory*// Gostechizdat (1952), pp. 1–180.

14. A. A. Karatsuba *Basics of analytic number theory*. URSS (2004), pp. 1–182.

15. T. Tao , V. Vu *Additive combinatorics*. Cambridge University Press 2006, pp. 1-530.

ФГУ ФНЦ Научно-исследовательский институт системных исследований Российской академии наук,
yuriisht@gmail.com
Получено 17.03.2017 г.
Принято в печать 12.06.2017 г.