On the estimates of Kloosterman sums. Small flowers to bouquet to jubilee

Maxim A. Korolev*

*Steklov Mathematical Institute (Moscow, Russia)

Vilnius Conference
in Combinatorics and Number Theory
2017, July 17 – 22

Introduction

Kloosterman sum $S_q(N) = S_q(N; a, b)$ modulo q of length N is the exponential sum of the type

$$S_q(N) = \sum_{1 \leqslant n \leqslant N}' e_q(a\overline{n} + bn), \qquad \overline{n}n \equiv 1 \pmod{q}$$

Usually we suppose that $(a, q) = 1$ or $(ab, q) = 1$.
Famous A.Weyl's bound (1948) and property of multiplicativity of Kloosterman sums imply non-trivial bound for $S_q(N)$ for

$$N \geqslant q^{0.5+\varepsilon}.$$

If $N \leqslant \sqrt{q}$, then $S_q(N)$ is called as a "short" sum.

1. Estimates of short sums

A.A.Karatsuba (1996): for any q,

$$S_q(N) \ll N\Delta_1, \quad \Delta_1 = \frac{1}{(\ln q)^c}, \quad q^{\varepsilon} \leqslant N \leqslant q^{4/7},\ c > 0$$

(in fact, $c = c(\varepsilon)$ was very small, $c(\varepsilon) \approx ([1/\varepsilon]!)^{-1}$).

M.K. (2000): for any q,

$$S_q(N) \ll N\Delta_2, \quad \Delta_2 = \frac{(\ln q)^{1/6}}{(\ln N)^{5/24}}(\ln\ln q)^5;$$

here

$$e^{(\ln q)^{\frac{4}{5}}(\ln\ln q)^5} \leqslant N \leqslant q^{\frac{4}{7}}$$

(in fact, $\tau(q)$ should not be very large here).

1. Estimates of short sums

J.Bourgain, M.Z.Garaev (2013): for prime q,

$$S_q(N) \ll N\Delta_3, \quad \Delta_3 = \frac{\ln q}{(\ln N)^{3/2}}\,(\ln\ln q)^2;$$

here

$$e^{(\ln q)^{\frac{2}{3}}(\ln\ln q)^2} \leqslant N \leqslant q^{\frac{4}{7}}.$$

Theorem 1. *For any prime q and*

$$e^{(\ln q)^{\frac{2}{3}}(\ln\ln q)^{\frac{4}{3}}} \leqslant N \leqslant \sqrt{q},$$

we have

$$\sum_{1\leqslant n\leqslant N} e_q(a\overline{n}) \ll N\,\Delta, \quad \Delta = \frac{\ln q}{(\ln N)^{3/2}}\,(\ln\ln q)^2.$$

1. Estimates of short sums

THEOREM 2. *For any prime* q *and*

$$e^{(\ln q)^{\frac{2}{3}}(\ln\ln q)^{\frac{1}{3}}} \leqslant N \leqslant \sqrt{q},$$

we have

$$\sum_{1\leqslant n\leqslant N} e_q(a\overline{n}) \ll N\,\frac{\ln D}{D}, \quad D = \frac{\ln N}{(\ln q)^{2/3}(\ln\ln q)^{1/3}}.$$

THEOREM 3. *For any prime* q *and*

$$e^{(\ln q)^{\frac{2}{3}}(\ln\ln q)^{\frac{1}{3}}} \leqslant N \leqslant \sqrt{q},$$

we have

$$\sum_{1\leqslant n\leqslant N} e_q(a\overline{n}+bn) \ll N\,D^{-3/4}, \quad D \quad \text{is the same as in Theorem 2.}$$

1. Estimates of short sums

Key ingredients:

(a) The estimate of $I_k(X)$:

$$\overline{p}_1 + \ldots + \overline{p}_k \equiv \overline{p}_{k+1} + \ldots + \overline{p}_{2k} \pmod{q},$$
$$k < X < p_j < X_1 \leqslant 2X.$$

A.A.Karatsuba:

$$I_k(X) \leqslant k! X^k, \quad \text{but only for} \quad k(2X)^{2k-1} < q.$$

J.Bourgain, M.Z.Garaev:

$$I_k(X) \ll k! X^k \biggl(\frac{k(2X)^{2k-1}}{q} + 1 \biggr).$$

1. Estimates of short sums

(b) Estimates of double sums over primes:

$$W_1 = \sum_{P<p\leqslant P_1} \sum_{R<r\leqslant R_1} F(p)G(r)e_q(a\overline{pr}),$$

$$W_2 = \sum_{P<p\leqslant P_1} \sum_{R<r\leqslant R_1} F(p)G(r)e_q(a\overline{pr}+bpr), \quad |F|, |G| \leqslant 1.$$

(c) The splitting of the set $\{n \leqslant N\}$ to two sets $\mathcal{A}$ and $\mathcal{B}$. All the numbers $n \in \mathcal{A}$ have at least two prime factors p and r from special intervals, and all the numbers $n \in \mathcal{B}$ have no such factors. The sum over $\mathcal{A}$ is estimated using the estimates of double sums, and the sum over $\mathcal{B}$ is estimated trivially: $|\mathcal{B}|$ (simple sieve etc.)

1. Estimates of short sums

Suppose $0 < \alpha < 0.5$ is fixed, and let $q \geqslant q_0(\alpha)$ be a prime, $N \asymp q^{\alpha}$. Then the estimates of Theorems 1 and 3 yields:

$$\sum_{n \leqslant N} e_q(a\overline{n}) \ll N \frac{(\ln \ln q)^2}{\sqrt{\ln q}},$$

$$\sum_{n \leqslant N} e_q(a\overline{n} + bn) \ll N \frac{(\ln \ln q)^{1/4}}{\sqrt[4]{\ln q}}.$$

Is it possible to improve these estimates?

1. Estimates of short sums

The estimates of the double sum has the form: $|W_1| \leqslant QR\Delta_1$, where

$$\Delta_1 = 2k^{\frac{1}{2s}} s^{\frac{1}{2k}} \left\{ \left(\frac{P^{k-1}}{\sqrt{q}} + \frac{\sqrt{q}}{P^k} \right) \cdot \left(\frac{R^{s-1}}{\sqrt{q}} + \frac{\sqrt{q}}{R^s} \right) \right\}^{\frac{1}{2ks}}$$

Suppose that k, s, P, R and $\varepsilon > 0$ satisfy

$$q^{\frac{1}{2k}+\varepsilon} \leqslant P \leqslant q^{\frac{1}{2(k-1)}-\varepsilon}, \quad q^{\frac{1}{2s}} \leqslant R \leqslant q^{\frac{1}{2(s-1)}}.$$

Then

$$\frac{P^{k-1}}{\sqrt{q}} + \frac{\sqrt{q}}{P^k} \leqslant 2q^{-\varepsilon(k-1)}, \quad \frac{R^{s-1}}{\sqrt{q}} + \frac{\sqrt{q}}{R^s} \leqslant 1$$

and

$$\Delta_1 \leqslant q^{-\delta}, \quad \delta = \frac{\varepsilon}{2s}\left(1 - \frac{1}{k}\right)$$

– estimate with power saving factor. If P, R both are close to the “**bad**” points of the type $q^{\frac{1}{2n}}$ then we have no good estimate.

1. Estimates of short sums

But if the length of the sum N is not very close to such a bad point $q^{\frac{1}{2n}}$, then the "bad" subset $\mathcal{B}$ becomes very thin!

THEOREM 4. *Let q be a prime, $k \geqslant 2$ is fixed, $0 < \alpha < 0.25$, and let $\varepsilon = \alpha/(k^2 - k)$. Then for any N such that*

$$q^{\frac{1}{2k}+\varepsilon} \leqslant N \leqslant q^{\frac{1}{2(k-1)}-\varepsilon}$$

one has

$$\sum_{n \leqslant N} e_q(a\overline{n} + bn) \ll N \frac{\ln \ln q}{\ln q}.$$

In particular, this bound holds for

$$q^{\frac{1}{4}+\varepsilon} \leqslant N \leqslant q^{\frac{1}{2}-\varepsilon}, \quad q^{\frac{1}{6}+\varepsilon} \leqslant N \leqslant q^{\frac{1}{4}-\varepsilon} \quad \text{etc.}$$

2. Kloosterman sums to powerful moduli

Suppose $q \geqslant 2$ be an integer, $d = \prod_{p|q} p$ is radical of q. Modulo q is called powerful if the fraction $\ln d / \ln q$ is small. The classic example is: $p \geqslant 2$ – fixed prime, $q = p^n$, $n \to +\infty$.

The observation of A.G.Postnikov (1955): in the case $q = p^n$, some problems (character sums, trigonometric sums with complicated functions in the exponent etc.) can be reduced to the estimates of exponential sums with polynomial.

Simplest example: Kloosterman sum modulo $q = p^n$:

$$(1 + px)^* \equiv 1 - px + (px)^2 - \ldots + (-1)^{n-1}(px)^{n-1} \pmod{p^n}$$

– polynomial in x of degree $n - 1$.

H.Iwaniec (1974) treated more general case of powerful moduli.

S.A.Stepanov and I.E.Shparlinski (1989) considered the generalization of Kloosterman sums with rational functions

$$\sideset{}{'}\sum_{c<n\leqslant c+N} e_q(F(n)/G(n)), \quad F(n)/G(n) \equiv F(n)\overline{G(n)} \pmod{q}.$$

2. Kloosterman sums to powerful moduli

THEOREM 5. *Suppose* $q \geqslant q_0$, $d = \mathrm{rad}\,(q)$, $\gamma = 160^{-4}$, $\gamma_1 = 900$, *and let*

$$\max\left\{d^{15}, e^{\gamma(\ln q)^{\frac{2}{3}}}\right\} \leqslant N \leqslant \sqrt{q}.$$

Then, for any a, b, c, *such that* $(a, q) = 1$, *we have:*

$$\Bigl|\sum_{c<n\leqslant c+N}{}^{'} e_q(a\overline{n} + bn)\Bigr| \leqslant N \exp\left(-\gamma\,\frac{(\ln N)^3}{(\ln q)^2}\right).$$

Key ingredients: (a) additive shift $n \mapsto n + xy$, (b) I.M.VINOGRADOV mean value theorem, (c) technic of H.IWANIEC.

2. Kloosterman sums to powerful moduli

In THEOREM 5, the radical d should be small in comparison with N: $d \leqslant N^{\frac{1}{15}}$. In some cases, one needs the estimates for lager d.

THEOREM 6. *Let* $0 < \delta < 0.05$ *be fixed,* $q \geqslant q_0(\delta)$,

$$\gamma = \frac{\delta^6}{2014}\left(\ln \frac{1}{\delta}\right)^{-2}, \quad \gamma_1 = \frac{1200}{\delta^2}\left(\ln \frac{1}{\delta}\right)^{\frac{2}{3}}.$$

and, finally, let

$$\max\left\{d^{2+\delta}, e^{\gamma(\ln q)^{\frac{2}{3}}}\right\} \leqslant N \leqslant q^{\frac{\delta}{20}}.$$

Then the estimate of THEOREM 5 *holds.*

3. "Intermediate case": moduli $q = p^r$ with fixed $r \geqslant 3$

Let r be a fixed natural number, $p \geqslant p_0(r)$ is prime and let $q = p^r$. In such case, we can use both J.G.VAN DER CORPUT's method and analogs of I.M.VINOGRADOV's method.

THEOREM 7. *Let* $r \geqslant 3$, $q = p^r$, $4p < N < N_1 \leqslant 2N \leqslant \sqrt{q}$, *then*

$$\sum_{N<n\leqslant N_1}{}' e_q(a\overline{n}) \ll N\left\{q^{-\alpha}(\ln q)^{\gamma} + \left(\frac{(q\ln q)^{\frac{1}{r-1}}}{N}\right)^{\beta}\right\}, \textit{where}$$

$$\alpha = \frac{1}{r(r^2-r+2)^2}, \quad \beta = \frac{r-1}{(r^2-r+2)^2+r-1},$$

$$\gamma = \frac{1}{(r^2-r+2)^2}.$$

For example, if $q = p^4$ then this bound is non-trivial for $N \geqslant q^{\frac{1}{3}+\varepsilon}$.

3. "Intermediate case": moduli $q = p^r$ with fixed $r \geqslant 3$

Key ingredients: I.M.Vinogradov's shift $n \mapsto n + xy$ and the estimate

$$J_{k,s}(X) \ll X^{\varepsilon}(X^k + X^{2k-\frac{1}{2}s(s+1)})$$

obtained by J.Bourgain, C.Demeter, L.Guth (2015).
Here $J_{k,s}(X)$ is the number of solutions of the system

$$\begin{cases} x_1 + \ldots + x_k = y_1 + \ldots + y_k, \\ \ldots \\ x_1^s + \ldots + x_k^s = y_1^s + \ldots + y_k^s, \end{cases}$$

with $1 \leqslant x_j, y_j \leqslant X$, $k, s > 1$ are any fixed integers; the factor X^{ε} can be removed if $k > 0.5s(s+1)$.

4. Kloosterman sums over primes

Let

$$T_q(N) = \sum_{n \leqslant N}{}' \Lambda(n) e_q(a\overline{n}).$$

P.Michel, E.Fouvry (1998): $T_q(N) \ll N^{1-\delta}$ for prime q and

$$q^{\frac{3}{4}+\varepsilon} \ll N \leqslant q$$

(here $\delta = \delta(\varepsilon) > 0$ is some constant; the precise value was not given by authors).

M.Z.Garaev (2010):

$$T_q(N) \ll q^{\varepsilon}(N^{\frac{15}{16}} + N^{\frac{2}{3}} q^{\frac{1}{4}}) q^{\varepsilon}$$

for the same q and N.

4. Kloosterman sums over primes

I.E.Shparlinski, R.Baker (2011): the same estimate, but for all $\boldsymbol{q}$

J.Bourgain (2009): $\boldsymbol{T_q(N) \ll N^{1-\delta}}$ for prime $\boldsymbol{q}$ and

$$\boldsymbol{q^{\frac{1}{2}+\varepsilon} \ll N \leqslant q}$$

R.Baker (2012): $\boldsymbol{\delta = 0.0005\,\varepsilon^4}$, for the same $\boldsymbol{N}$ and composite $\boldsymbol{q}$ with small "quadratic part".

Thus, the shortest sum in the case of arbitrary $\boldsymbol{q}$ has the length $\boldsymbol{N \geqslant q^{\frac{3}{4}+\varepsilon}}$.

Theorem 8. *For any* $\boldsymbol{q}$ *and* $\boldsymbol{q^{0.7+\varepsilon} \ll N \leqslant q}$ *we have*

$$\boldsymbol{T_q(N) \ll N\Delta, \quad \Delta = \left(q^7 N^{-10}\right)^{\frac{1}{74}} q^{\varepsilon}.}$$

4. Kloosterman sums over primes

THEOREM 9. *Let* p *be a prime,* $q = p^4$ *and let* $q^{0.6+\varepsilon} \leqslant N \leqslant q$. *Then* $T_q(N) \ll N\Delta$, *where*

$$\Delta = q^{-0.3\,\varepsilon} + (q^3 N^{-5})^{\frac{1}{231}} q^{0.006\,\varepsilon}.$$

THEOREM 10. *Let* p *be a prime,* $r \geqslant 5$, $q = p^r$ *and let* $0 < \varepsilon < (2/r)^2$. *Then, for*

$$q^{\frac{2}{r-1}+\varepsilon} \ll N \leqslant q,$$

we have: $T_q(N) \ll Nq^{-\delta}$, $\delta = \varepsilon/(2r)^3$.

Key ingredients: (a) Theorem 8 and (b) I.M.VINOGRADOV - R.VAUGHAN identity.

5. Kloosterman sums over Pyatetski-Shapiro sequences

Let $c > 1$, $c \notin \mathbb{Z}$ be a fixed constant. Then the sequence

$$\mathbb{N}_c = \{m = [n^c],\ n = 1, 2, 3, \ldots\}$$

is called *Pyatetski-Shapiro sequence* in honour of I.I. Pyatetskii-Shapiro. In 1953, he proved that the set $\mathbb{N}_c$ contains infinitely many primes for any fixed $c \in (1, c_0)$ with $c_0 = \frac{12}{11} = 1.090909\ldots$.

Moreover, he established that

$$\pi_c(N) = \#\{p \in \mathbb{N}_c,\ p \text{ is prime},\ p \leqslant N\} \sim \frac{N^{\gamma}}{\ln N}, \quad \gamma = \frac{1}{c}.$$

Now this result is known for $c_0 = \frac{243}{205} = 1.18536\ldots$ (J. Rivat, J. Wu, 2001).

5. Kloosterman sums over Pyatetski-Shapiro sequences

Different arithmetic properties of $\mathbb{N}_c$:

The largest prime factor of $[n^c]$ for infinitely many $n \geqslant 1$, squarefree and "smooth" numbers in $\mathbb{N}_c$; Carmichael numbers with prime factors from $\mathbb{N}_c$: (G.N. Arkhipov, V.N. Chubarikov, 1997; R.C. Baker, W. Banks, J. Brudern, I.E. Shparlinskii, A.J. Weingartner, 2013)

Squares in $\mathbb{N}_c$ (K. Liu, I.E. Shparlinskii, T.P. Zhang)

Additive problems with numbers from $\mathbb{N}_c$ (A. Balog, J. Friedlander, D. Tolev, M. Laporta, S.V. Konyagin, S.A. Gritsenko, M.Z. Garaev, Ka-Lam Kueh, Zh. Petrov et all).

Least quadratic non-residue $n_c(p)$ to prime modulus p (W.D. Banks, M.Z. Garaev, D.R. Heath-Brown, I.E. Shparlinskii).

5. Kloosterman sums over Pyatetski-Shapiro sequences

The problem is to estimate the sum:

$$S_q(c;N) = \sum_{1 \leqslant n \leqslant N} e_q\bigl(a[n^c]^*\bigr), \quad 1 < c < c_0.$$

Two aspects of this problem:

1) To make the domain $c \in (1, c_0)$ as wide as possible;

2) To make the length N of the sum as short as possible.

These aspects suppress each other: the dilation of $(1, c_0)$ leads to the increasing of N, and the decreasing of N leads to small interval $(1, c_0)$.
Our aim is to make the sum $S = S_q(c;N)$ more shorter.

5. Kloosterman sums over Pyatetski-Shapiro sequences

THEOREM 11. *Let q be a prime and suppose that (κ,λ) is an exponential pair and let $\varrho = \kappa+\lambda+\frac{1}{2}$. Then $|S| \ll N\Delta$, where*

$$\Delta = \left(\frac{q^{h(c)}}{N}\right)^{\theta(c)} + \left(\frac{q^{h_1(c)}}{N}\right)^{\theta_1(c)},$$

and

$$h(c) = \frac{2c+\varrho-1}{c(2+\varrho)-c^2\varrho-1}$$

(h_1, θ, θ_1 are the functions os the same type).

This estimate is non-trivial if $N \gg q^{h(c)+\varepsilon}$. To make N small, we should minimize $h(c)$. The pair $\kappa = \frac{32}{205}, \lambda = \frac{32}{205}$ leads to

$$\min_{c>1} h(c) = 2-\delta, \quad \delta = 0.191538\ldots, \quad c_0 = 1.0504145\ldots.$$

5. Kloosterman sums over Pyatetski-Shapiro sequences

The main difficulty: sum over “small n”. Simplification of the problem: replace the sum $S_q(c;N)$ by

$$W_q(c;N) = \sum_{N<n\leqslant N_1} e_q\bigl(a[n^c]^*\bigr), \quad N \asymp N_1.$$

THEOREM 12. *If q is prime,*

$$N \geqslant q^{1+\varepsilon}$$

then

$$W_q(c;N) \ll N^{1-\delta}$$

for $1 < c < 1+\delta_0$ where δ, δ_0 depends on ε.

5. Kloosterman sums over Pyatetski-Shapiro sequences

THEOREM 13. *If p is prime and $q = p^2$,*

$$N \geqslant q^{\frac{3}{4}+\varepsilon}$$

then

$$W_q(c; N) \ll N^{1-\delta}$$

for $1 < c < 1 + \delta_0$ where δ, δ_0 depends on ε.

THEOREM 14. *The same result holds true for*

$$q = p^3, \quad N \geqslant q^{\frac{1}{2}+\varepsilon}; \quad q = p^4, \quad N \geqslant q^{\frac{1}{3}+\varepsilon} \quad \text{etc.}$$

Thank you very much for attention!