Exponential Sums and their Applications

by

N. M. Korobov

Department of Mathematics,
Moscow University,
Moscow, U.S.S.R.

KLUWER ACADEMIC PUBLISHERS
DORDRECHT / BOSTON / LONDON

Mathematics and Its Applications (*Soviet Series*)

Volume 80

Exponential Sums and their Applications

by

N. M. Korobov
Department of Mathematics,
Moscow University,
Moscow, U.S.S.R.

KLUWER ACADEMIC PUBLISHERS
DORDRECHT / BOSTON / LONDON

Library of Congress Cataloging-in-Publication Data

Korobov, N. M. (Nikolaĭ Mikhaĭlovich)
[Trigonometricheskie summy i ikh prilozhenii͡a. English]
Exponential sums and their applications / N.M. Korobov ;
[translated by Yu.N Shakhov].
p. cm. -- (Mathematics and its applications. Soviet series ;
v. 80)
Translation of: Trigonometricheskie summy i ikh prilozhenii͡a.
Includes bibliographical references and index.
ISBN 0-7923-1647-9 (printed on acid free paper)
1. Trigonometric sums. 2. Exponential sums. I. Title.
II. Series: Mathematics and its applications (Kluwer Academic
Publishers). Soviet series : v. 80.
QA246.8.T75K6713 1992
512'.73--dc20 92-1223
ISBN 0-7923-1647-9

Published by Kluwer Academic Publishers,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

Kluwer Academic Publishers incorporates
the publishing programmes of
D. Reidel, Martinus Nijhoff, Dr W. Junk and MTP Press.

Sold and distributed in the U.S.A. and Canada
by Kluwer Academic Publishers,
101 Philip Drive, Norwell, MA 02061, U.S.A.

In all other countries, sold and distributed
by Kluwer Academic Publishers Group,
P.O. Box 322, 3300 AH Dordrecht, The Netherlands.

Printed on acid-free paper

Translated by Yu. N. Shakhov

This book is the translation of the original work
Trigonometrical Sums and their Applications
© Nauka, Moscow 1989

Printed in the Netherlands

SERIES EDITOR'S PREFACE

'Et moi, ..., si j'avait su comment en revenir, je n'y serais point allé.'
Jules Verne

The series is divergent; therefore we may be able to do something with it.
O. Heaviside

One service mathematics has rendered the human race. It has put common sense back where it belongs, on the topmost shelf next to the dusty canister labelled 'discarded nonsense'.
Eric T. Bell

Mathematics is a tool for thought. A highly necessary tool in a world where both feedback and nonlinearities abound. Similarly, all kinds of parts of mathematics serve as tools for other parts and for other sciences.

Applying a simple rewriting rule to the quote on the right above one finds such statements as: 'One service topology has rendered mathematical physics ...'; 'One service logic has rendered computer science ...'; 'One service category theory has rendered mathematics ...'. All arguably true. And all statements obtainable this way form part of the raison d'être of this series.

This series, *Mathematics and Its Applications*, started in 1977. Now that over one hundred volumes have appeared it seems opportune to reexamine its scope. At the time I wrote

> "Growing specialization and diversification have brought a host of monographs and textbooks on increasingly specialized topics. However, the 'tree' of knowledge of mathematics and related fields does not grow only by putting forth new branches. It also happens, quite often in fact, that branches which were thought to be completely disparate are suddenly seen to be related. Further, the kind and level of sophistication of mathematics applied in various sciences has changed drastically in recent years: measure theory is used (non-trivially) in regional and theoretical economics; algebraic geometry interacts with physics; the Minkowsky lemma, coding theory and the structure of water meet one another in packing and covering theory; quantum fields, crystal defects and mathematical programming profit from homotopy theory; Lie algebras are relevant to filtering; and prediction and electrical engineering can use Stein spaces. And in addition to this there are such new emerging subdisciplines as 'experimental mathematics', 'CFD', 'completely integrable systems', 'chaos, synergetics and large-scale order', which are almost impossible to fit into the existing classification schemes. They draw upon widely different sections of mathematics."

By and large, all this still applies today. It is still true that at first sight mathematics seems rather fragmented and that to find, see, and exploit the deeper underlying interrelations more effort is needed and so are books that can help mathematicians and scientists do so. Accordingly MIA will continue to try to make such books available.

If anything, the description I gave in 1977 is now an understatement. To the examples of interaction areas one should add string theory where Riemann surfaces, algebraic geometry, modular functions, knots, quantum field theory, Kac-Moody algebras, monstrous moonshine (and more) all come together. And to the examples of things which can be usefully applied let me add the topic 'finite geometry'; a combination of words which sounds like it might not even exist, let alone be applicable. And yet it is being applied: to statistics via designs, to radar/sonar detection arrays (via finite projective planes), and to bus connections of VLSI chips (via difference sets). There seems to be no part of (so-called pure) mathematics that is not in immediate danger of being applied. And, accordingly, the applied mathematician needs to be aware of much more. Besides analysis and numerics, the traditional workhorses, he may need all kinds of combinatorics, algebra, probability, and so on.

In addition, the applied scientist needs to cope increasingly with the nonlinear world and the extra mathematical sophistication that this requires. For that is where the rewards are. Linear models are honest and a bit sad and depressing: proportional efforts and results. It is in the nonlinear world that infinitesimal inputs may result in macroscopic outputs (or vice versa). To appreciate what I am hinting at: if electronics were linear we would have no fun with transistors and computers; we would have no TV; in fact you would not be reading these lines.

There is also no safety in ignoring such outlandish things as nonstandard analysis, superspace and anticommuting integration, p-adic and ultrametric space. All three have applications in both electrical engineering and physics. Once, complex numbers were equally outlandish, but they frequently proved the shortest path between 'real' results. Similarly, the first two topics named have already provided a number of 'wormhole' paths. There is no telling where all this is leading - fortunately.

Thus the original scope of the series, which for various (sound) reasons now comprises five subseries: white (Japan), yellow (China), red (USSR), blue (Eastern Europe), and green (everything else), still applies. It has been enlarged a bit to include books treating of the tools from one subdiscipline which are used in others. Thus the series still aims at books dealing with:

- a central concept which plays an important role in several different mathematical and/or scientific specialization areas;
- new applications of the results and ideas from one area of scientific endeavour into another;
- influences which the results, problems and concepts of one field of enquiry have, and have had, on the development of another.

The method of exponential sums is one of the few general methods in (analytic and 'elementary') number theory. It is also, without a doubt, one of the more powerful ones. Getting acquainted with it, and learning to appreciate its ideas and applicability, is a bit of a problem though. The standard sources were composed by and for expert analytic number theorists.

The present monograph gives a straightforward accessible account of the theory with a number of illustrative applications (to number theory, but also to numerical questions). At the same time it contains some new results (in theory) and new applications due to the author.

The main aim of this series is to improve understanding between different mathematical specialisms. In my opinion this book contributes nontrivially to that.

The shortest path between two truths in the real domain passes through the complex domain.
J. Hadamard

La physique ne nous donne pas seulement l'occasion de résoudre des problèmes ... elle nous fait pressentir la solution.
H. Poincaré

Never lend books, for no one ever returns them; the only books I have in my library are books that other folk have lent me.
Anatole France

The function of an expert is not to be more right than other people, but to be wrong for more sophisticated reasons.
David Butler

Bussum, 9 February 1992

Michiel Hazewinkel

CONTENTS

PREFACE

The method of exponential sums is one of a few general methods enabling us to solve a wide range of miscellaneous problems from the theory of numbers and its applications. The strongest results have been obtained with the aid of this method. Therefore knowledge of the fundamentals of the theory of exponential sums is necessary for studying modern number theory.

The study of the method of exponential sums is complicated by the fact that the well-known monographs [44], [16] and [17] are intended for experts, embrace a large number of the fundamental problems at once, are written briefly and for these reasons are not really suitable for a first acquaintance with the subject.

The main aim of the present monograph is to present an as simple as possible exposition of the fundamentals of the theory and, with a series of examples, to show how exponential sums arise and are applied in problems of number theory and in questions connected with their applications. First of all, the book is intended for those who are beginning a study of exponential sums. At the same time, it can be interesting for specialists also, because it contains some results which are not included in other monographs.

This book represents an expanded course of the lectures delivered by the author at the Mechanics and Mathematics Department of Moscow University during the course of many years. It contains the classical results of Gauss, and the methods of Weyl, Mordell and Vinogradov, which are exposed in detail; the traditional applications of exponential sums to the distribution of fractional parts, the estimation of the Riemann zeta-function, the theory of congruences and Diophantine equations are considered too. Some new applications of exponential sums are also included in the book. In particular, questions relating to the distribution of digits in periodic fractions, arising in the expansion of rational numbers under an arbitrary base notation, are considered, and a number of results concerning the completely uniform distribution of fractional parts and the approximate computation of multiple integrals are discussed.

Questions concerning the additive theory of numbers are not included in the book, because for their real understanding one should master the fundamentals of the theory of exponential sums. It will be easier to become acquainted with these and other questions exposed in the monographs [44], [17], [47], [6] and [43] following a subsequent, more profound study of the subject.

To read this book it is sufficient to know the fundamentals of mathematical analysis and to have a knowledge of elementary number theory. For those, who are coming to grips with the subject for the first time, it is recommended to combine the reading of this book with solving problems concerning the investigation and application of the simplest exponential sums [45].

INTRODUCTION

An *exponential sum* is defined as a sum of the form

$$S(P)=\sum_{x} e^{2\pi i\, f(x)}, \qquad (1)$$

where x runs over all integers (or some of them) from a certain interval, P is the number of the summands and $f(x)$ is an arbitrary function taking on real values under integer x. Many problems of the number theory and its applications can be reduced to the study of such sums.

Let us show, for instance, how exponential sums arise in solving the problem of possibility to represent a natural number N in the form of a sum of integer powers of natural numbers, the exponents being equal,

$$N=x_1^n+\ldots+x_k^n \qquad (2)$$

(Waring's problem). Let n and k be fixed positive integers, P the greatest integer not exceeding $N^{\frac{1}{n}}$ and $T_k(N)$ the number of solutions of the equation (2). For an integer a, let the function $\psi(a)$ be defined by means of the equality

$$\psi(a)=\int_0^1 e^{2\pi i\, a\alpha}d\alpha=\begin{cases}1 & \text{if} \quad a=0,\\ 0 & \text{if} \quad a\neq 0.\end{cases}$$

Then obviously

$$T_k(N)=\sum_{x_1,\ldots,x_k=1}^{P}\psi(x_1^n+\ldots+x_k^n-N)=\sum_{x_1,\ldots,x_k=1}^{P}\int_0^1 e^{2\pi i\,(x_1^n+\ldots+x_k^n-N)\alpha}d\alpha$$
$$=\int_0^1 e^{-2\pi i\,\alpha N}\left(\sum_{x=1}^{P}e^{2\pi i\,\alpha x^n}\right)^k d\alpha.$$

Thus thc arithmetic problem concerning the number of solutions of the equation (2) is reduced to the study of integral depending on the power of the exponential sum

$$S(P)=\sum_{x=1}^{P}e^{2\pi i\,\alpha x^n}. \qquad (3)$$

For applications, the most important sums are those, for which the function $f(x)$ is a polynomial and the summation domain is an interval:

$$S(P)=\sum_{x=Q+1}^{Q+P} e^{2\pi i f(x)}, \qquad f(x)=\alpha_1 x+\ldots+\alpha_n x^n. \tag{4}$$

Such exponential sums are called *Weyl's sums* and the degree of the polynomial $f(x)$ *the degree of the Weyl's sum*. So, for example, the sum (3), arising in Waring's problem, is a Weyl's sum of degree n.

The main problem of the theory of exponential sums is to obtain an upper estimate of the modulus of an exponential sum as sharp as possible. As the modulus of every addend of the sum is equal to unity, so for any sum (1), the following trivial estimate is valid:

$$|S(P)| \leqslant P.$$

The first general nontrivial estimates were given by H. Weyl [49]. Under certain requirements for the leading coefficient of the polynomial $f(x)$, he showed that under any ε from the interval $0<\varepsilon<1$ there holds the estimate

$$\left|\sum_{x=1}^{P} e^{2\pi i f(x)}\right| \leqslant C(n,\varepsilon)P^{1-\frac{\gamma}{2^{n-1}}}, \tag{5}$$

where $\gamma = 1-\varepsilon$ and $C(n,\varepsilon)$ does not depend on P. Under $n \geqslant 12$ the essential improvement of this result was obtained by I. M. Vinogradov [44], who showed that in the estimate (5) under certain $\gamma > 0$ the right-hand side $C(n,\varepsilon)P^{1-\frac{\gamma}{2^{n-1}}}$ might be replaced by the quantity $C(n)P^{1-\frac{\gamma}{n^2\log n}}$.

If fractional parts of function $f(x)$ have an integer period, i.e., if under a certain positive integer τ the equality $\{f(x+\tau)\}=\{f(x)\}$, where $\{f(x)\}$ is the fractional part of the function $f(x)$, holds for any integer x, then the sum

$$S(\tau)=\sum_{x=1}^{\tau} e^{2\pi i f(x)}$$

is called a *complete exponential sum*. As an example of a complete exponential sum we can take the Weyl's sum, in which all coefficients of the polynomial $f(x)$ are rational and the number of summands is equal to the common denominator of the coefficients:

$$S(q)=\sum_{x=1}^{q} e^{2\pi i \frac{a_1x+\ldots+a_nx^n}{q}}. \tag{6}$$

Under $a_n \not\equiv 0 \pmod q$ such sums are called *complete rational sums of degree n*. There are more precise estimates of these sums, than estimates of Weyl's sums of the general form.

The thorough research of complete rational sums of the second degree was carried out by Gauss. In particular, he showed that under $(a,q)=1$ for the modulus of the sum

$$S(q)=\sum_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}}$$

the equalities

$$|S(q)|=\begin{cases}\sqrt{q} & \text{if } q\equiv 1 \pmod 2,\\ \sqrt{2q} & \text{if } q\equiv 0 \pmod 4,\\ 0 & \text{if } q\equiv 2 \pmod 4)\end{cases}$$

are valid.

For complete rational sums of an arbitrary degree under a prime q Mordell [36] obtained the estimate

$$\left|\sum_{x=1}^{q} e^{2\pi i \frac{a_1x+\ldots+a_nx^n}{q}}\right| \leqslant C(n)q^{1-\frac{1}{n}}, \tag{7}$$

where $C(n)$ does not depend on q. Hua Loo-Keng [17] extended this estimation to the case of an arbitrary positive integer q. An essential improvement of the Mordell's result was got by A. Weil [48], who showed that under a prime q the modulus of the sum (7) does not exceed the quantity $(n-1)\sqrt{q}$. Under fixed n and increasing q the estimates by A. Weil and Hua Loo-Keng are the best possible, apart from the values of the constants, and do not admit further essential improvement.

Another example of complete sums, different from the complete rational sum (6), is a sum with exponential function

$$S(\tau)=\sum_{x=1}^{\tau} e^{2\pi i \frac{aq^x}{m}}, \tag{8}$$

where $(q,m)=1$ and τ is the order of q for modulus m. The problem of the number of occurrences of a fixed block of digits in the first P digits of a periodical fraction, arising under q-adic expansion of an arbitrary rational number $\frac{b}{m}$, is reduced to estimations of sums (8) and sums $S(P)$ for $P\leqslant\tau$ [32]. The magnitude of the sum (8) depends on the characterization of prime factorization of m and it turns out that for complete sums this magnitude is equal to zero in most cases. But if $P<\tau$, then under $n=\frac{\log m}{\log P}$ and m being equal to a power of a prime, the estimate

$$\left|\sum_{x=1}^{P} e^{2\pi i \frac{aq^x}{m}}\right| \leqslant CP^{1-\frac{\gamma}{n^2}},$$

where C and γ are absolute constants, holds.

The necessity to estimate exponential sums arises in the problem of approximate computation of integrals of an arbitrary multiplicity [23] as well. Let us consider, for instance, a quadrature formula constructed by means of an arbitrary net $M_k = M(\xi_1(k), \xi_2(k))$ $(k = 1, 2, \dots, P)$

$$\int_0^1\int_0^1 F(x_1, x_2)\, dx_1 dx_2 = \frac{1}{P}\sum_{k=1}^{P} F(\xi_1(k), \xi_2(k)) - R_P[F], \tag{9}$$

where $F(x_1, x_2)$ is a periodic function given by its absolutely convergent Fourier expansion

$$F(x_1, x_2) = \sum_{m_1, m_2=-\infty}^{\infty} C(m_1, m_2) e^{2\pi i(m_1 x_1 + m_2 x_2)}.$$

Substituting the series into equality (9) we get after interchanging the order of summation

$$R_P[F] = \frac{1}{P} \sum_{m_1, m_2=-\infty}^{\infty}{}' C(m_1, m_2) \sum_{k=1}^{P} e^{2\pi i(m_1\xi_1(k) + m_2\xi_2(k))},$$

where $\sum'$ denotes the summation over all $(m_1, m_2) \neq (0, 0)$. Hence the error term in the quadrature formula (9) satisfies

$$|R_P[F]| \leqslant \frac{1}{P} \sum_{m_1, m_2=-\infty}^{\infty}{}' |C(m_1, m_2)|\, |S(m_1, m_2)|,$$

where the exponential sum

$$S(m_1, m_2) = \sum_{k=1}^{P} e^{2\pi i(m_1\xi_1(k) + m_2\xi_2(k))}$$

is determined by the introduction of the net $M(\xi_1(k), \xi_2(k))$. Choosing the functions $\xi_1(k)$ and $\xi_2(k)$ so that the sums $S(m_1, m_2)$ could be estimated sufficiently well, we get the opportunity to construct quadrature formulas of high precision.

Chapter I of this book contains a detailed exposition of some elementary knowledge from the theory of complete exponential sums and sums, which estimations are reduced to estimations of complete sums. Theorems treated in the chapter are comparatively simple, but they constitute the base of the theory of exponential sums of the general form and serve as a necessary preparation to more complicated constructions of Chapter II. To illustrate possible applications of complete sums, the solution of the problem concerning the distribution of digits in the period of fractions, arising in representing rational numbers under an arbitrary base notation, is given in Chapter I.

A technique used in Chapter II is much more complicated than in Chapter I. Chapter II is devoted to an exposition of the theory of Weyl's sums of the general form.

In the chapter, the fundamental methods by Weyl and Vinogradov are presented as well as researches based on the repeated application of the mean value theorem; their applications to estimation of sums, arising in the Riemann zeta-function theory [25]–[28], are given also.

In Chapter III, the exponential sums applications to the distribution of fractional parts and the construction of quadrature formulas are considered. The Weyl theory of uniform distribution is exposed, the questions of complete uniform distribution [20] and their connection with the theory of normal numbers [22] are also considered there. The final part of the chapter is devoted to the problem of approximate calculation of multiple integrals and to construction of interpolation formulas for functions of many variables [23], [29], and [30].

CHAPTER I

COMPLETE EXPONENTIAL SUMS

§ 1. Sums of the first degree

The simplest example of Weyl's sums is the sum of the first degree

$$S(P) = \sum_{x=Q+1}^{Q+P} e^{2\pi i\,\alpha x}.$$

This sum pertains to a number of a few exponential sums, which can be not only estimated but evaluated immediately. In fact, if α is an integer, then $e^{2\pi i\,\alpha} = 1$ and therefore

$$\sum_{x=Q+1}^{Q+P} e^{2\pi i\,\alpha x} = P.$$

But if α is not an integer, then $e^{2\pi i\,\alpha} \neq 1$, and, summing the geometric progression, we have

$$\sum_{x=Q+1}^{Q+P} e^{2\pi i\,\alpha x} = \frac{e^{2\pi i\,\alpha P} - 1}{e^{2\pi i\,\alpha} - 1}\, e^{2\pi i\,\alpha(Q+1)}. \tag{10}$$

But usually it is more convenient to use not these exact equalities but the following estimate:

LEMMA 1. *Let α be an arbitrary real number, Q an integer, and P a positive integer. Then*

$$\left| \sum_{x=Q+1}^{Q+P} e^{2\pi i\,\alpha x} \right| \leqslant \min\left(P, \frac{1}{2\|\alpha\|}\right), \tag{11}$$

where $\|\alpha\|$ is the distance from α to the nearest integer.

Proof. Since the both sides of (11) are even periodic functions of α with period 1, then it suffices to prove the estimate (11) for $0 \leqslant \alpha \leqslant \frac{1}{2}$. Observing that over this interval

$$\left|e^{2\pi i\,\alpha} - 1\right| = 2\sin \pi\alpha \geqslant 4\alpha = 4\|\alpha\|,$$

then under $\alpha \neq 0$ from the equality (10) we get

$$\left|\sum_{x=Q+1}^{Q+P} e^{2\pi i\,\alpha x}\right| = \frac{|e^{2\pi i\,\alpha P}-1|}{|e^{2\pi i\,\alpha}-1|} \leqslant \frac{1}{2\|\alpha\|}\,.$$

For $\frac{1}{2P} \leqslant \alpha \leqslant \frac{1}{2}$ using this estimate and for $0 \leqslant \alpha < \frac{1}{2P}$ applying the trivial estimate

$$\left|\sum_{x=Q+1}^{Q+P} e^{2\pi i\,\alpha x}\right| \leqslant P,$$

we obtain the assertion of the lemma.

Let a be an arbitrary integer and q a positive integer. We define the function $\delta_q(a)$ with the help of the equality

$$\delta_q(a) = \begin{cases} 1 & \text{if } \ a \equiv 0 \pmod q, \\ 0 & \text{if } \ a \not\equiv 0 \pmod q. \end{cases}$$

In the next lemma the connection between this function and complete rational sums of the first degree will be established.

LEMMA 2. *For any integer a and any positive integer q we have the equality*

$$\delta_q(a) = \frac{1}{q}\sum_{x=1}^{q} e^{2\pi i\,\frac{ax}{q}}. \tag{12}$$

Proof. If $a \equiv 0 \pmod q$, then

$$\frac{1}{q}\sum_{x=1}^{q} e^{2\pi i\,\frac{ax}{q}} = \frac{1}{q}\sum_{x=1}^{q} 1 = 1.$$

Now let $a \not\equiv 0 \pmod q$. Then we get

$$\frac{1}{q}\sum_{x=1}^{q} e^{2\pi i\,\frac{ax}{q}} = \frac{1}{q}\,\frac{e^{2\pi i\,a}-1}{e^{2\pi i\,\frac{a}{q}}-1}\,e^{2\pi i\,\frac{a}{q}} = 0.$$

The assertion of the lemma obviously follows from these equalities and the definition of $\delta_q(a)$.

The function $\delta_q(x)$ will be used in the further exposition permanently. Its importance is determined by the fact that it enables us to establish the connection between the exponential sums' investigation and the question of the number of solutions of congruences.

Let us consider, for instance, the question of the number of solutions of the congruence

$$x_1^n + \ldots + x_k^n \equiv \lambda \pmod q, \tag{13}$$

that is analogous to the question of the number of solutions of Waring's equation (2), which was mentioned in the introduction. We denote the number of solutions of this congruence, as the variables $x_1, \ldots, x_k$ run through complete sets of residues to modulus q independently, by $T(\lambda)$. Obviously, by virtue of the definition of the function $\delta_q(x)$

$$T(\lambda) = \sum_{x_1,\ldots,x_k=1}^{q} \delta_q(x_1^n + \ldots + x_k^n - \lambda).$$

Hence it follows by Lemma 2 that

$$\begin{aligned} T(\lambda) &= \sum_{x_1,\ldots,x_k=1}^{q} \frac{1}{q}\sum_{a=1}^{q} e^{2\pi i\,\frac{a(x_1^n+\ldots+x_k^n-\lambda)}{q}} \\ &= \frac{1}{q}\sum_{a=1}^{q} e^{-2\pi i\,\frac{a\lambda}{q}} \sum_{x_1,\ldots,x_k=1}^{q} e^{2\pi i\,\frac{a(x_1^n+\ldots+x_k^n)}{q}} \\ &= \frac{1}{q}\sum_{a=1}^{q} e^{-2\pi i\,\frac{a\lambda}{q}} \left(\sum_{x=1}^{q} e^{2\pi i\,\frac{ax^n}{q}}\right)^k. \end{aligned}$$

Thus the number of solutions of the congruence (13) is represented in terms of complete rational exponential sums

$$S(a,\,q) = \sum_{x=1}^{q} e^{2\pi i\,\frac{ax^n}{q}}.$$

We expose some properties of the function $\delta_q(x)$, which follow from its definition immediately.

1°. The function $\delta_q(x)$ is periodic. Its period is equal to q.

2°. If $(a,\,q) = 1$ and b is an arbitrary integer, then the equalities

$$\delta_q(ax) = \delta_q(x),$$

$$\sum_{x=1}^{q} \delta_q(ax+b) = 1$$

are valid.

3°. Under any positive integer q_1, the equalities

$$\delta_{q_1 q}(q_1 x) = \delta_q(x), \qquad \sum_{y=1}^{q_1} \delta_{q_1 q}(x+qy) = \delta_q(x)$$

hold.

4°. If $(q_1, q) = 1$, then the equality

$$\delta_{q_1 q}(x) = \delta_{q_1}(x)\delta_q(x)$$

is valid.

5°. Under any positive integer P, which does not exceed q, we have

$$\sum_{y=1}^{P} \delta_q(x-y) = \begin{cases} 1 & \text{if} \quad 1 \leqslant x \leqslant P, \\ 0 & \text{if} \quad P < x \leqslant q. \end{cases} \tag{14}$$

LEMMA 3. *Let q be an arbitrary positive integer, $1 \leqslant a < q$, and $(a, q) = 1$. Then the estimates*

$$\sum_{x=1}^{q-1} \frac{1}{\left\|\frac{ax}{q}\right\|} \leqslant 2q \log q,$$

$$\sum_{x=1}^{q-1} \frac{1}{x\left\|\frac{ax}{q}\right\|} \leqslant 18\, M \log^2 q,$$

where M is the largest among the partial quotients of the simple continued fraction of the number $\frac{a}{q}$, hold.

Proof. Let m be an arbitrary positive integer. Under $x \geqslant 1$ using the inequality

$$\frac{1}{x} \leqslant \log(2x+1) - \log(2x-1),$$

we obtain

$$\sum_{1\leqslant x\leqslant m} \frac{1}{x} \leqslant \sum_{1\leqslant x\leqslant m} \log(2x+1) - \sum_{1\leqslant x\leqslant m} \log(2x-1) = \log(2m+1).$$

Hence under odd and even q, respectively, it follows that

$$\sum_{x=1}^{\frac{q-1}{2}} \frac{1}{x} \leqslant \log q, \qquad \sum_{x=1}^{\frac{q-2}{2}} \frac{1}{x} \leqslant \log(q-1) \leqslant -\frac{1}{q} + \log q. \tag{15}$$

Since the function $\|\frac{ax}{q}\|$ is periodic with period q and $(a, q) = 1$, then under odd q according to (15) we get

$$\sum_{x=1}^{q-1} \frac{1}{\left\|\frac{ax}{q}\right\|} = \sum_{x=1}^{q-1} \frac{1}{\left\|\frac{x}{q}\right\|} = 2\sum_{x=1}^{\frac{q-1}{2}} \frac{1}{\left\|\frac{x}{q}\right\|} = 2q \sum_{x=1}^{\frac{q-1}{2}} \frac{1}{x} \leqslant 2q \log q.$$

But the same estimate is obtained by (15) under even q as well:

$$\sum_{x=1}^{q-1} \frac{1}{\left\|\frac{ax}{q}\right\|} = 2 + 2q \sum_{x=1}^{\frac{q-2}{2}} \frac{1}{x} \leqslant 2q \log q.$$

The first assertion of the lemma is proved.

To prove the second assertion we shall apply the Abel summation formula

$$\sum_{x=1}^{q-1} u_x v_x = u_q \sum_{x=1}^{q-1} v_x + \sum_{m=1}^{q-1} \left(u_m - u_{m+1}\right) \sum_{x=1}^{m} v_x.$$

Under $u_x = \frac{1}{x}$ and $v_x = \frac{1}{\|\frac{ax}{q}\|}$ we obtain

$$\sum_{x=1}^{q-1} \frac{1}{x\left\|\frac{ax}{q}\right\|} = \frac{1}{q} \sum_{x=1}^{q-1} \frac{1}{\left\|\frac{ax}{q}\right\|} + \sum_{m=1}^{q-1} \frac{1}{m(m+1)} \sum_{x=1}^{m} \frac{1}{\left\|\frac{ax}{q}\right\|}. \tag{16}$$

Let the expansion of the number $\frac{a}{q}$ in simple continued fraction be

$$\frac{a}{q} = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_n}}}.$$

Then under $\nu = 1, 2, \ldots, n$ the following equalities take place:

$$\frac{a}{q} = \frac{P_\nu}{Q_\nu} + \frac{\theta_\nu}{Q_\nu^2} \qquad (|\theta_\nu| \leqslant 1), \tag{17}$$

where P_ν and Q_ν are relatively prime, $1 = Q_0 \leqslant Q_1 < \ldots < Q_n = q$, $Q_\nu \leqslant (q_\nu + 1)Q_{\nu-1} \leqslant 2MQ_{\nu-1}$.

If $1 \leqslant m < \frac{1}{2}q$, then determining ν from the condition

$$\frac{1}{2} Q_{\nu-1} \leqslant m < \frac{1}{2} Q_\nu$$

and using the equality (17), we get

$$\left\|\frac{ax}{q}\right\| = \left\|\frac{P_\nu x}{Q_\nu} + \frac{\theta_\nu x}{Q_\nu^2}\right\| \geqslant \left\|\frac{P_\nu x}{Q_\nu}\right\| - \left\|\frac{\theta_\nu x}{Q_\nu^2}\right\|. \tag{18}$$

Since under $1 \leqslant x < \frac{1}{2}Q_\nu$ we have

$$\left\|\frac{\theta_\nu x}{Q_\nu^2}\right\| \leqslant \frac{1}{2Q_\nu} \leqslant \frac{1}{2}\left\|\frac{P_\nu x}{Q_\nu}\right\|,$$

hence from (18) it follows that

$$\left\| \frac{ax}{q} \right\| \geqslant \frac{1}{2} \left\| \frac{P_\nu x}{Q_\nu} \right\|.$$

Then using the first inequality of the lemma, we obtain

$$\begin{aligned} \sum_{x=1}^{m} \frac{1}{\left\| \frac{ax}{q} \right\|} &\leqslant 2 \sum_{x=1}^{Q_\nu - 1} \frac{1}{\left\| \frac{P_\nu x}{Q_\nu} \right\|} \leqslant 4 Q_\nu \log Q_\nu \\ &\leqslant 8 M Q_{\nu-1} \log q \leqslant 16 M m \log q. \end{aligned} \tag{19}$$

But if $\frac{1}{2} q \leqslant m < q$, then

$$\sum_{x=1}^{m} \frac{1}{\left\| \frac{ax}{q} \right\|} \leqslant \sum_{x=1}^{q-1} \frac{1}{\left\| \frac{ax}{q} \right\|} \leqslant 2 q \log q \leqslant 4 m \log q,$$

and, therefore, the estimate (19) holds not only for $m < \frac{1}{2} q$, but for any $m < q$ as well. Substituting it into the equality (16), we get the second assertion of the lemma:

$$\sum_{x=1}^{q-1} \frac{1}{x \left\| \frac{ax}{q} \right\|} \leqslant 2 \log q + \sum_{m=1}^{q-1} \frac{16 M \log q}{m+1} \leqslant 18 M \log^2 q.$$

Now we'll show how these lemmas, containing quite a little information concerning exponential sums, enable us to get nontrivial arithmetic results.

Let $(a, q) = 1$, $P_1 \leqslant q$, $P_2 \leqslant q$, and T be the number of solutions of the congruence

$$a x_1 \equiv x_2 \pmod q, \qquad 1 \leqslant x_1 \leqslant P_1,\ 1 \leqslant x_2 \leqslant P_2. \tag{20}$$

If P_1 or P_2 equals q, then, evidently,

$$T = \frac{1}{q} P_1 P_2.$$

The question becomes more complicated, if both P_1 and P_2 are less than q. In this case, it can be shown that

$$T = \frac{1}{q} P_1 P_2 + 9 \theta M \log^2 q, \qquad |\theta| \leqslant 1, \tag{21}$$

where M is the largest among partial quotients of the simple continued fraction of the number $\frac{a}{q}$.

Really, using Lemma 2, we obtain

$$T = \sum_{x_1=1}^{P_1} \sum_{x_2=1}^{P_2} \delta_q(a x_1 - x_2) = \frac{1}{q} \sum_{x_1=1}^{P_1} \sum_{x_2=1}^{P_2} \sum_{x=1}^{q} e^{2\pi i \frac{(a x_1 - x_2) x}{q}}.$$

Hence, after singling out the summand with $x = q$, it follows that

$$T = \frac{1}{q} P_1 P_2 + R, \tag{22}$$

where

$$\begin{aligned} |R| &= \frac{1}{q} \left| \sum_{x=1}^{q-1} \left(\sum_{x_1=1}^{P_1} e^{2\pi i \frac{a x x_1}{q}} \right) \left(\sum_{x_2=1}^{P_2} e^{-2\pi i \frac{x x_2}{q}} \right) \right| \\ &\leqslant \frac{1}{q} \sum_{x=1}^{q-1} \left| \sum_{x_1=1}^{P_1} e^{2\pi i \frac{a x x_1}{q}} \right| \left| \sum_{x_2=1}^{P_2} e^{2\pi i \frac{x x_2}{q}} \right|. \end{aligned}$$

Thus the problem concerning the number of solutions of the congruence (20) is reduced to the problem of the estimation of Weyl's sums of the first degree. Using Lemma 1 and observing that $\| \frac{x}{q} \|$ and $\| \frac{ax}{q} \|$ are even periodic functions with period q, we get

$$\begin{aligned} |R| &\leqslant \frac{1}{q} \sum_{x=1}^{q-1} \min \left(P_1, \frac{1}{2 \left\| \frac{ax}{q} \right\|} \right) \min \left(P_2, \frac{1}{2 \left\| \frac{x}{q} \right\|} \right) \\ &\leqslant \frac{1}{4q} \sum_{1 \leqslant |x| \leqslant \frac{1}{2} q} \frac{1}{\left\| \frac{x}{q} \right\| \left\| \frac{ax}{q} \right\|} = \frac{1}{2} \sum_{1 \leqslant x \leqslant \frac{1}{2} q} \frac{1}{x \left\| \frac{ax}{q} \right\|}. \end{aligned}$$

Hence according to Lemma 3 it follows that

$$|R| \leqslant 9 M \log^2 q,$$

and by (22) this estimate is equivalent to the equality (21).

§ 2. General properties of complete sums

As it was said above, the sum

$$S(\tau) = \sum_{x=1}^{\tau} e^{2\pi i f(x)} \tag{23}$$

is called a complete exponential sum, if under any integer x for fractional parts of the function $f(x)$, the equality $\{ f(x + \tau) \} = \{ f(x) \}$ is satisfied.

We shall expose some examples of complete sums. Let $a_1, \dots, a_n$ be integers and $\varphi(x) = a_1 x + \dots + a_n x^n$. Since, obviously,

$$(x+q)^\nu \equiv x^\nu \pmod q \qquad (\nu = 1, 2, \dots, n),$$

then the following congruences hold:

$$\sum_{\nu=1}^{n} a_\nu (x+q)^\nu \equiv \sum_{\nu=1}^{n} a_\nu x^\nu \pmod q,$$
$$\varphi(x+q) \equiv \varphi(x) \pmod q.$$

But then under any integer x

$$\left\{\frac{\varphi(x+q)}{q}\right\} = \left\{\frac{\varphi(x)}{q}\right\},$$

and, therefore, the sum

$$S(q) = \sum_{x=1}^{q} e^{2\pi i \frac{\varphi(x)}{q}} = \sum_{x=1}^{q} e^{2\pi i \frac{a_1 x + \dots + a_n x^n}{q}},$$

which was called a complete rational sum in the introduction, is a complete exponential sum in the sense of the definition (23).

Now let us consider a sum with exponential function

$$S(\tau) = \sum_{x=1}^{\tau} e^{2\pi i \frac{aq^x}{m}}, \tag{24}$$

where $(a,m) = 1$, $(q,m) = 1$ and τ is the order of q for modulus m. Let q^{-1} denote the solution of the congruence $qx \equiv 1 \pmod m$. Then using the congruence $q^\tau \equiv 1 \pmod m$, under any integer x we obtain

$$\left\{\frac{aq^{x+\tau}}{m}\right\} = \left\{\frac{aq^x}{m}\right\}.$$

Therefore τ is a period of fractional parts of the function $\frac{aq^x}{m}$ and the sum (24) is a complete exponential sum.

Expose some properties of complete sums, which follow from the definition directly.

1°. The magnitude of the complete exponential sum (23) will not change, if the summation variable runs through any complete set of residues to modulus τ instead of the interval $[1, \tau]$.

Really, since $\{f(x+\tau)\} = \{f(x)\}$, then under $x \equiv y \pmod \tau$ the equality $\{f(x)\} = \{f(y)\}$ holds. But then

$$e^{2\pi i f(x)} = e^{2\pi i f(y)}$$

and the totality of the summands of the sum (23) is independent of whichever complete set of incongruent residues to modulus τ is run by the summation variable.

2°. If $(\lambda, \tau) = 1$, μ is an integer and n is a positive integer, then for complete sums the equalities

$$\sum_{x=1}^{\tau} e^{2\pi i f(x)} = \sum_{x=1}^{\tau} e^{2\pi i f(\lambda x + \mu)}, \tag{25}$$
$$\sum_{x=1}^{n\tau} e^{2\pi i f(x)} = n \sum_{x=1}^{\tau} e^{2\pi i f(x)} \tag{26}$$

hold.

The first among these equalities is a particular case of the property 1°, because under $(\lambda, \tau) = 1$ the linear function $\lambda x + \mu$ runs through a complete set of residues to modulus τ, when x runs through a complete residue set to modulus τ. The second equality follows from 1° as well, for under varying from 1 to $n\tau$ the summation variable runs n times through complete residue set to modulus τ.

3°. If sums

$$\sum_{x=1}^{\tau} e^{2\pi i f_1(x)} \quad \text{and} \quad \sum_{x=1}^{\tau} e^{2\pi i f_2(x)} \tag{27}$$

are complete, then the sum

$$\sum_{x=1}^{\tau} e^{2\pi i (f_1(x) + f_2(x))} \tag{28}$$

is complete also.

Really, it follows from completeness of the sums (27), that fractional parts of the functions $f_1(x)$ and $f_2(x)$ have the same period τ:

$$\{f_1(x+\tau)\} = \{f_1(x)\}, \qquad \{f_2(x+\tau)\} = \{f_2(x)\}.$$

But then

$$\{f_1(x+\tau) + f_2(x+\tau)\} = \{f_1(x) + f_2(x)\}$$

and, therefore, the sum (28) is a complete exponential sum.

THEOREM 1 (multiplication formula). *Let under integers x*

$$\{f(x)\} = \{f_1(x) + \dots + f_s(x)\}, \tag{29}$$

where fractional parts of the functions $f_1(x), \dots, f_s(x)$ are periodic and their periods $\tau_1, \dots, \tau_s$ are relatively prime to each other. Then the equality

$$\sum_{x=1}^{\tau_1 \dots \tau_s} e^{2\pi i f(x)} = \prod_{\nu=1}^{s} \sum_{x_\nu=1}^{\tau_\nu} e^{2\pi i f_\nu(x_\nu)} \tag{30}$$

holds.

Proof. Since by the assumption

$$\{f_\nu(x+\tau_\nu)\} = \{f_\nu(x)\} \qquad (\nu = 1,2,\ldots,s) \tag{31}$$

and by (29)

$$\{f(x+\tau_1\ldots\tau_s)\} = \{f(x)\},$$

then all the exponential sums in the equality (30) are complete. Let variables $x_1,\ldots,x_s$ run independently through complete residue sets to moduli $\tau_1,\ldots,\tau_s$, respectively. Since the $\tau_1,\ldots,\tau_s$ are coprime, then the sum

$$x_1\tau_2\ldots\tau_s + \ldots + \tau_1\ldots\tau_{s-1}x_s$$

runs through a complete residue set to modulus $\tau_1\ldots\tau_s$, and, therefore,

$$\sum_{x=1}^{\tau_1\ldots\tau_s} e^{2\pi i\, f(x)} = \sum_{x_1=1}^{\tau_1}\cdots\sum_{x_s=1}^{\tau_s} e^{2\pi i\, f(x_1\tau_2\ldots\tau_s+\ldots+\tau_1\ldots\tau_{s-1}x_s)}. \tag{32}$$

Since by (29) and (31)

$$\{f(x_1\tau_2\ldots\tau_s+\ldots+\tau_1\ldots\tau_{s-1}x_s)\} = \{f_1(x_1\tau_2\ldots\tau_s)+\ldots+f_s(\tau_1\ldots\tau_{s-1}x_s)\},$$

then the equality (32) may be rewritten in the form

$$\sum_{x=1}^{\tau_1\ldots\tau_s} e^{2\pi i\, f(x)} = \sum_{x_1=1}^{\tau_1}\cdots\sum_{x_s=1}^{\tau_s} e^{2\pi i\,(f_1(x_1\tau_2\ldots\tau_s)+\ldots+f_s(\tau_1\ldots\tau_{s-1}x_s))}.$$

Hence, using the property (25), we obtain the multiplication formula:

$$\sum_{x=1}^{\tau_1\ldots\tau_s} e^{2\pi i\, f(x)} = \sum_{x_1=1}^{\tau_1}\cdots\sum_{x_s=1}^{\tau_s} e^{2\pi i\,(f_1(x_1)+\ldots+f_s(x_s))} = \prod_{\nu=1}^{s}\sum_{x_\nu=1}^{\tau_\nu} e^{2\pi i\, f_\nu(x_\nu)}.$$

In a number of cases, the multiplication formula simplifies the study of complete sums. As an example of that we shall consider complete rational sums.

Let $\varphi(x) = a_1x+\ldots+a_nx^n$ be an arbitrary polynomial with integral coefficients, $q = p_1^{\alpha_1}\ldots p_s^{\alpha_s}$ prime factorization of q, and numbers $b_1,\ldots,b_n$ be chosen to satisfy the congruence

$$1 \equiv b_1p_2^{\alpha_2}\ldots p_s^{\alpha_s}+\ldots+p_1^{\alpha_1}\ldots p_{s-1}^{\alpha_{s-1}}b_s \pmod q. \tag{33}$$

Then for complete rational sums the following equality holds

$$\sum_{x=1}^{q} e^{2\pi i\,\frac{\varphi(x)}{q}} = \prod_{\nu=1}^{s}\sum_{x_\nu=1}^{p_\nu^{\alpha_\nu}} e^{2\pi i\,\frac{b_\nu\varphi(x_\nu)}{p_\nu^{\alpha_\nu}}}. \tag{34}$$

Really, since

$$\left\{\frac{\varphi(x+q)}{q}\right\} = \left\{\frac{\varphi(x)}{q}\right\}, \qquad \left\{\frac{b_\nu\varphi(x+p_\nu^{\alpha_\nu})}{p_\nu^{\alpha_\nu}}\right\} = \left\{\frac{b_\nu\varphi(x)}{p_\nu^{\alpha_\nu}}\right\} \qquad (1\leqslant\nu\leqslant s)$$

and by (33)

$$\left\{\frac{\varphi(x)}{q}\right\} = \left\{\frac{b_1\varphi(x)}{p_1^{\alpha_1}}+\ldots+\frac{b_s\varphi(x)}{p_s^{\alpha_s}}\right\},$$

then applying Theorem 1, we obtain the equality (34).

The multiplication formula (34) reduces the investigation of complete rational sums with an arbitrary denominator q to the investigation of simpler sums with a denominator being a power of a prime.

As another example on the multiplication formula we shall prove the equality

$$\sum_{x=1}^{q-1} e^{2\pi i\,\frac{x^2}{q}} = (1-i^q)\sum_{x=1}^{q-1} e^{2\pi i\,\frac{x^2}{4q}}, \qquad q\equiv 1 \pmod 2, \tag{35}$$

which will be needed later in studying Gaussian sums. Consider the sum

$$S = \sum_{x=1}^{4q} e^{2\pi i\,\frac{x^2}{4q}}.$$

Single out the summands, for which x is a multiple of q, and group the others in four sums:

$$\begin{aligned} S &= \sum_{x=1}^{4} e^{2\pi i\,\frac{qx^2}{4}} + \sum_{x=1}^{q-1}\left(e^{2\pi i\,\frac{x^2}{4q}} + e^{2\pi i\,\frac{(2q-x)^2}{4q}} + e^{2\pi i\,\frac{(2q+x)^2}{4q}} + e^{2\pi i\,\frac{(4q-x)^2}{4q}}\right) \\ &= \sum_{x=1}^{4} e^{2\pi i\,\frac{qx^2}{4}} + 4\sum_{x=1}^{q-1} e^{2\pi i\,\frac{x^2}{4q}}. \end{aligned} \tag{36}$$

On the other hand, according to the multiplication formula

$$S = \sum_{x_1=1}^{4} e^{2\pi i\,\frac{b_1x_1^2}{4}}\sum_{x_2=1}^{q} e^{2\pi i\,\frac{b_2x_2^2}{q}},$$

where b_1 and b_2 satisfy the congruence $qb_1+4b_2 \equiv 1 \pmod{4q}$. Since this congruence is satisfied under $b_1 = q$ and $b_2 = \frac{1}{4}(1-q^2)$, then after singling out the summand with $x_2 = q$ and replacing x_2 by $2x$, we obtain

$$\begin{aligned} S &= \sum_{x_1=1}^{4} e^{2\pi i\,\frac{b_1x_1^2}{4}} + \sum_{x_1=1}^{4} e^{2\pi i\,\frac{b_1x_1^2}{4}}\sum_{x=1}^{q-1} e^{2\pi i\,\frac{4b_2x^2}{q}} \\ &= \sum_{x=1}^{4} e^{2\pi i\,\frac{qx^2}{4}} + \sum_{x_1=1}^{4} e^{2\pi i\,\frac{qx_1^2}{4}}\sum_{x=1}^{q-1} e^{2\pi i\,\frac{x^2}{q}}. \end{aligned} \tag{37}$$

Now observing that

$$\sum_{x_1=1}^{4} e^{2\pi i \frac{q x_1^2}{4}} = 2(1+i^q),$$

from (36) and (37) we get the equality (35):

$$\sum_{x=1}^{q-1} e^{2\pi i \frac{x^2}{q}} = \frac{4}{2(1+i^q)} \sum_{x=1}^{q-1} e^{2\pi i \frac{x^2}{4q}} = (1-i^q) \sum_{x=1}^{q-1} e^{2\pi i \frac{x^2}{4q}}.$$

Now we shall consider a certain class of exponential sums, whose nontrivial estimates can be easily obtained by the reduction of the problem to the estimation of complete sums.

Let fractional parts of a function $f(x)$ be periodic, their least period be equal to τ, $1 \leqslant P < \tau$ and Q an arbitrary integer. Then the sum

$$S(P) = \sum_{x=Q+1}^{Q+P} e^{2\pi i f(x)} \tag{38}$$

is called an *incomplete exponential sum.*

THEOREM 2. *For any incomplete exponential sum $S(P)$ defined by the equality* (38), *the estimate*

$$|S(P)| \leqslant \max_{1 \leqslant a \leqslant \tau} \left| \sum_{x=1}^{\tau} e^{2\pi i (f(x) + \frac{ax}{\tau})} \right| (1 + \log \tau)$$

holds.

Proof. From the property (14) of the function $\delta_q(x)$ it follows that under $P \leqslant \tau$

$$\sum_{y=Q+1}^{Q+P} \delta_\tau(x-y) = \begin{cases} 1 & \text{if} \quad Q+1 \leqslant x \leqslant Q+P, \\ 0 & \text{if} \quad Q+P < x \leqslant Q+\tau. \end{cases}$$

Applying this discontinuous factor and using Lemma 2, we obtain

$$\sum_{x=Q+1}^{Q+P} e^{2\pi i f(x)} = \sum_{x=Q+1}^{Q+\tau} e^{2\pi i f(x)} \sum_{y=Q+1}^{Q+P} \delta_\tau(x-y)$$
$$= \frac{1}{\tau} \sum_{a=1}^{\tau} \left(\sum_{y=Q+1}^{Q+P} e^{-2\pi i \frac{ay}{\tau}} \right) \sum_{x=Q+1}^{Q+\tau} e^{2\pi i \left(f(x) + \frac{ax}{\tau}\right)}.$$

Since fractional parts of the functions $f(x)$ and $\frac{ax}{\tau}$ have period τ, then by (28) the latter sum in this equality is complete and, therefore,

$$\sum_{x=Q+1}^{Q+P} e^{2\pi i f(x)} = \frac{1}{\tau} \sum_{a=1}^{\tau} \left(\sum_{y=Q+1}^{Q+P} e^{-2\pi i \frac{ay}{\tau}} \right) \sum_{x=1}^{\tau} e^{2\pi i \left(f(x) + \frac{ax}{\tau}\right)}.$$

Hence, using Lemmas 2 and 3, we get the theorem assertion:

$$\left| \sum_{x=Q+1}^{Q+P} e^{2\pi i f(x)} \right| \leqslant \frac{1}{\tau} \sum_{a=1}^{\tau} \left| \sum_{x=1}^{\tau} e^{2\pi i \left(f(x) + \frac{ax}{\tau}\right)} \right| \min\left(P, \frac{1}{2\|\frac{a}{\tau}\|}\right)$$
$$\leqslant \frac{1}{\tau} \max_{1 \leqslant a \leqslant \tau} \left| \sum_{x=1}^{\tau} e^{2\pi i \left(f(x) + \frac{ax}{\tau}\right)} \right| \sum_{a=1}^{\tau} \min\left(P, \frac{1}{2\|\frac{a}{\tau}\|}\right)$$
$$\leqslant \max_{1 \leqslant a \leqslant \tau} \left| \sum_{x=1}^{\tau} e^{2\pi i \left(f(x) + \frac{ax}{\tau}\right)} \right| (1 + \log \tau).$$

§ 3. Gaussian sums

A *Gaussian sum* is a complete rational exponential sum of the second degree

$$S(q) = \sum_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}},$$

where q is an arbitrary positive integer and $(a, q) = 1$. Gaussian sums as well as the first degree sums considered in the first paragraph can be evaluated precisely. We shall start with a comparatively simple question about the evaluation of the modulus of such sums.

THEOREM 3. *For the modulus of the Gaussian sum, the following equalities hold true:*

$$|S(q)| = \begin{cases} \sqrt{q} & \text{if} \quad q \equiv 1 \pmod 2, \\ \sqrt{2q} & \text{if} \quad q \equiv 0 \pmod 4, \\ 0 & \text{if} \quad q \equiv 2 \pmod 4. \end{cases}$$

Proof. Let the complex conjugate of the sum $S(q)$ be denoted by $\overline{S}(q)$. Then we get

$$|S(q)|^2 = \overline{S}(q) S(q) = \sum_{y=1}^{q} e^{-2\pi i \frac{ay^2}{q}} \sum_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}}.$$

Utilize the second property of complete sums and replace x by $x+y$ in the inner sum. Then after interchanging the order of summation, we obtain

$$|S(q)|^2 = \sum_{x=1}^{q} \sum_{y=1}^{q} e^{2\pi i \frac{a(x+y)^2 - ay^2}{q}} = \sum_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}} \sum_{y=1}^{q} e^{2\pi i \frac{2axy}{q}}.$$

Hence by Lemma 2 it follows that

$$|S(q)|^2 = q\sum_{x=1}^{q} e^{2\pi i\frac{ax^2}{q}}\delta_q(2ax). \tag{39}$$

Since a and q are coprime by the statement, then under odd q the only nonzero summand of the right-hand side of this equality is the summand obtained under $x = q$, and therefore

$$|S(q)|^2 = qe^{2\pi i\frac{aq^2}{q}} = q. \tag{40}$$

But if q is even, then in the sum (39) there are two nonzero summands which are obtained under $x = \frac{1}{2}q$ and $x = q$. Therefore, observing that under even q, from $(a,q) = 1$ it follows that a is odd, we get

$$|S(q)|^2 = q\left(e^{2\pi i\frac{aq}{4}}+1\right) = q\left(e^{2\pi i\frac{q}{4}}+1\right) = \begin{cases} 2q & \text{if } q\equiv 0 \pmod 4,\\ 0 & \text{if } q \equiv 2 \pmod 4.\end{cases}$$

The theorem assertion follows from this equality and (40).

Note that in the case of odd q, the assertion of Theorem 3 is valid for sums of the general form, too.

Indeed, let us show that under $(2a_2, q) = 1$ the equality

$$\left|\sum_{x=1}^{q} e^{2\pi i\frac{a_1x+a_2x^2}{q}}\right| = \sqrt{q} \tag{41}$$

holds. Choose b satisfying the congruence $2a_2b \equiv a_1 \pmod q$. Then obviously

$$a_1x + a_2x^2 \equiv a_2(x+b)^2 - a_2b^2 \pmod q$$

and, therefore,

$$\sum_{x=1}^{q} e^{2\pi i\frac{a_1x+a_2x^2}{q}} = e^{-2\pi i\frac{a_2b^2}{q}}\sum_{x=1}^{q} e^{2\pi i\frac{a_2(x+b)^2}{q}}.$$

Hence we obtain the equality (41):

$$\left|\sum_{x=1}^{q} e^{2\pi i\frac{a_1x+a_2x^2}{q}}\right| = \left|\sum_{x=1}^{q} e^{2\pi i\frac{a_2(x+b)^2}{q}}\right| = \sqrt{q}.$$

Let as consider the simplest properties of Gaussian sums. We shall assume that $q = p$, where $p > 2$ is a prime. It is easy to show that under $a = 0 \pmod p$ the following equality holds:

$$\sum_{x=1}^{p} e^{2\pi i\frac{ax^2}{p}} = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{ax}{p}}, \tag{42}$$

where $\left(\frac{x}{p}\right)$ is Legendre's symbol. Indeed, if x varies from 1 to $p-1$, then x^2 runs twice through values of quadratic residues of p, and since

$$1+\left(\frac{x}{p}\right) = \begin{cases} 2 & \text{if } x \text{ is a quadratic residue,}\\ 0 & \text{if } x \text{ is a quadratic non-residue,}\end{cases}$$

then

$$\sum_{x=1}^{p} e^{2\pi i\frac{ax^2}{p}} = 1+\sum_{x=1}^{p-1} e^{2\pi i\frac{ax^2}{p}} = 1+\sum_{x=1}^{p-1}\left[1+\left(\frac{x}{p}\right)\right]e^{2\pi i\frac{ax}{p}}.$$

Hence observing that by Lemma 2 under $a = 0 \pmod p$

$$1+\sum_{x=1}^{p-1} e^{2\pi i\frac{ax}{p}} = p\delta_p(a) = 0,$$

we obtain the equality (42).

Now we shall show that under $a = 0 \pmod p$

$$\sum_{x=1}^{p} e^{2\pi i\frac{ax^2}{p}} = \left(\frac{a}{p}\right)\sum_{x=1}^{p} e^{2\pi i\frac{x^2}{p}}. \tag{43}$$

Indeed, multiplying the equality (42) by $\left(\frac{a^2}{p}\right) = 1$ and observing that ax runs through a complete set of residues prime to p when x runs through such a set, we get

$$\sum_{x=1}^{p} e^{2\pi i\frac{ax^2}{p}} = \left(\frac{a}{p}\right)\sum_{x=1}^{p-1}\left(\frac{ax}{p}\right)e^{2\pi i\frac{ax}{p}} = \left(\frac{a}{p}\right)\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{x}{p}}.$$

The equality (43) follows, because by (42)

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{x}{p}} = \sum_{x=1}^{p} e^{2\pi i\frac{x^2}{p}}.$$

Next we shall show that knowing the modulus of a Gaussian sum it is easy to evaluate its value to within the accuracy of the sign. Indeed, let

$$S(p) = \sum_{x=1}^{p} e^{2\pi i\frac{x^2}{p}}.$$

Then, using the equality (43), we get

$$\overline{S}(p) = \sum_{x=1}^{p} e^{-2\pi i\frac{x^2}{p}} = \left(\frac{-1}{p}\right)\sum_{x=1}^{p} e^{2\pi i\frac{x^2}{p}} = \left(\frac{-1}{p}\right)S(p).$$

Hence after multiplying by $(\frac{-1}{p})S(p)$ it follows that

$$S^2(p) = \left(\frac{-1}{p}\right)|S(p)|^2 = \left(\frac{-1}{p}\right)p.$$

Now, since $(\frac{-1}{p})$ takes on the value 1 under $p \equiv 1 \pmod 4$ and the value -1 under $p \equiv 3 \pmod 4$, we obtain

$$S(p) = \begin{cases} \pm\sqrt{p} & \text{if} \quad p \equiv 1 \pmod 4, \\ \pm i\sqrt{p} & \text{if} \quad p \equiv 3 \pmod 4. \end{cases} \tag{44}$$

The question about choosing the proper sign in these equalities is more difficult. Its solution was found by Gauss. A comparatively simple proof of the Gauss theorem given in the paper [9] is exposed below.

THEOREM 4. *Under any odd prime p the following equalities are valid*:

$$\sum_{x=1}^{p} e^{2\pi i \frac{x^2}{p}} = \begin{cases} \sqrt{p} & \textit{if} \quad p \equiv 1 \pmod 4, \\ i\sqrt{p} & \textit{if} \quad p \equiv 3 \pmod 4. \end{cases}$$

Proof. Let us show at first that

$$\left| \sum_{\sqrt{p}<x<p} e^{2\pi i \frac{x^2}{4p}} \right| < \sqrt{p}. \tag{45}$$

Indeed, apply Abel's summation formula

$$\sum_{x=q+1}^{p-1} (u_x - u_{x-1})v_x = \sum_{x=q+1}^{p-1} u_x(v_x - v_{x+1}) + u_{p-1}v_p - u_q v_{q+1} \tag{46}$$

under $q = [\sqrt{p}]$ and

$$u_x = e^{2\pi i \frac{x(x+1)}{4p}}, \qquad v_x = \frac{1}{\sin \pi \frac{x}{2p}}.$$

Since, obviously,

$$u_{p-1}v_p = e^{2\pi i \frac{p-1}{4}} = (-1)^{\frac{p-1}{2}}$$

and

$$u_x - u_{x-1} = e^{2\pi i \frac{x^2}{4p}} \left(e^{2\pi i \frac{x}{4p}} - e^{-2\pi i \frac{x}{4p}} \right) = 2ie^{2\pi i \frac{x^2}{4p}} \sin \pi \frac{x}{2p},$$

then from (46) it follows that

$$2i \sum_{\sqrt{p}<x<p} e^{2\pi i \frac{x^2}{4p}} = \sum_{x=q+1}^{p-1} e^{2\pi i \frac{x(x+1)}{4p}} \left(\frac{1}{\sin \pi \frac{x}{2p}} - \frac{1}{\sin \pi \frac{x+1}{2p}} \right) + (-1)^{\frac{p-1}{2}} - \frac{e^{2\pi i \frac{q(q+1)}{4p}}}{\sin \pi \frac{q+1}{2p}}.$$

But then, observing that under $1 \leqslant x \leqslant p-1$

$$\left| \frac{1}{\sin \pi \frac{x}{2p}} - \frac{1}{\sin \pi \frac{x+1}{2p}} \right| = \frac{1}{\sin \pi \frac{x}{2p}} - \frac{1}{\sin \pi \frac{x+1}{2p}},$$

we get

$$2\left| \sum_{\sqrt{p}<x<p} e^{2\pi i \frac{x^2}{4p}} \right| \leqslant \sum_{x=q+1}^{p-1} \left(\frac{1}{\sin \pi \frac{x}{2p}} - \frac{1}{\sin \pi \frac{x+1}{2p}} \right) + 1 + \frac{1}{\sin \pi \frac{q+1}{2p}} = \frac{2}{\sin \pi \frac{q+1}{2p}}.$$

Since

$$\frac{2}{\sin \pi \frac{q+1}{2p}} \leqslant \frac{2p}{q+1} < 2\sqrt{p},$$

the estimate (45) follows.

Now, observing that

$$\operatorname{Re}(1-i) \sum_{1 \leqslant x < \sqrt{p}} e^{2\pi i \frac{x^2}{4p}} = \sum_{1 \leqslant x < \sqrt{p}} \left(\cos \pi \frac{x^2}{2p} + \sin \pi \frac{x^2}{2p} \right) > \sqrt{p} - 1,$$

and using the estimate (45), we get

$$\operatorname{Re}(1-i) \sum_{x=1}^{p-1} e^{2\pi i \frac{x^2}{4p}} \geqslant \operatorname{Re}(1-i) \sum_{1 \leqslant x < \sqrt{p}} e^{2\pi i \frac{x^2}{4p}} - \left| (1-i) \sum_{\sqrt{p}<x<p} e^{2\pi i \frac{x^2}{4p}} \right| > \sqrt{p} - 1 - \sqrt{2}\sqrt{p} > -\sqrt{p}. \tag{47}$$

Let $p \equiv 1 \pmod 4$. Then by (44)

$$\sum_{x=1}^{p} e^{2\pi i \frac{x^2}{p}} = \pm\sqrt{p}, \tag{48}$$