Tatra Mt. Math. Publ. **20** (2000), 155–162

Tatra Mountains
Mathematical Publications

SUMS OF CHARACTERS WITH PRIME NUMBERS AND THEIR APPLICATIONS

Anatolij A. Karatsuba

ABSTRACT. We give estimates for sums of summands of the form

$$\chi\big(f(p)\big)\,,\tau_k(n)\chi\big(f(n)\big)\,,$$

where $p \le N$, p are prime numbers, $f(x) = x + a, f(x) = (x + a)(x + b)$, χ is a non-principal Dirichlet character modulo q, and $ab(a - b) \not\equiv 0\ (q)$.

§ 1. This is an extended version of a lecture delivered by the author at the 14th Czech–Slovak International Conference, September 6–10, 1999, Liptovský Sv. Ján. The author expresses his deep gratitute to Prof. K. Nemoga for his hospitality and to Prof. W. Narkiewicz for acting as interpreter.

§ 2. The lecture is devoted to a branch of analytic number theory, where a substantial use is made of a result obtained by methods of algebraic geometry. Basic contributions to the development of this branch are due to I. M. Vinogradov and the author (see [1]–[22]).

§ 3. By methods of algebraic geometry, a theorem has been proved which is an analogue of the Riemann hypothesis for so called congruence zeta-functions. Particular cases of this theorem were proved by Hasse, the general case by A. Weil, and higher-dimensional generalizations by Deligne.

§ 4. A corollary of it was the following theorem on estimates for sums of characters: Let ψ be a multiplicative character of the field $\mathbb{F}_q$, having order $m > 1$, and let $f \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree, which is not the mth power of other polynomial. If d is the number of distinct roots of the polynomial f in its splitting field over $\mathbb{F}_q$, then for every $a \in \mathbb{F}_q$ one has the inequality

$$\left|\sum_{c\in\mathbb{F}_q}\Psi\big(af(c)\big)\right| \le (d-1)\sqrt{q}\,. \tag{1}$$

2000 Mathematics Subject Classification: Primary 11L05; Secondary 11K06.
Keywords: sums of characters; trigonometric sums.

Translated by Július Korbaš.

(see, e.g., [23; p. 279]).

It is the estimate (1) that applies in analytic number theory. It is called the Hasse–Weil estimate.

§ 5. For the remainder of the paper we shall be assuming that q is a prime number and that $\psi = \chi$ is a non-principal Dirichlet character mod q. Then §3 and §4 imply that for $N < q$ one has the inequality

$$\left| \sum_{x=1}^{N} \chi\big(f(x)\big) \right| \le (d-1)\sqrt{q}\,\log q\,. \tag{2}$$

§ 6. Note that the imply (2) for $f(x) = x + a$ was obtained as early as in 1914 by I. M. Vinogradov in his degree work when graduating from the university, and later by Polya (see [1]–[3]). This estimate is now called Vinogradov's or Vinogradov–Polya's (estimate of a sum of characters).

§ 7. The inequality (2) implies a number of arithmetic results on quadratic residues and non-residues, primitive roots, indices, modulo q in sequences of the form $f(x)$, $x = 1, 2, \dots N$, where $N \ge \sqrt{q}\,(\log q)^{1+\varepsilon}$, $\varepsilon > 0$, $q \to +\infty$. Results of this type are well known, and we shall not comment on them in detail.

§ 8. But one may ask another question here: What happens if the values of x are assumed to be not consecutive natural numbers but instead, for instance, consecutive primes? Clearly, we are arriving at the question of upper bounds for $|S_N|$, where

$$S_N = \sum_{p \le N} \chi\big(f(p)\big)\,, \tag{3}$$

and p assumes values of consecutive primes. The sum S_N is essentially different from the sum over consecutive positive integers. Consecutive positive integers are repeated modulo q. This is not the case for prime numbers, and that causes the complexity of the study of S_N. A trivial estimate of $|S_N|$ is the following:

$$|S_N| \le \pi(N)\,,$$

where $\pi(N)$ is the number of primes not exceeding N.

§ 9. The problem of estimating $|S_N|$ was posed by I. M. Vinogradov in 1937. By the method used by I. M. Vinogradov to solve the Goldbach problem, he proved in 1938 the following theorem (see [4]): Let $f(x) = x + a$, $a \not\equiv 0 \pmod{q}$, $N \ge q^{1+\varepsilon}$, $\varepsilon > 0$, $q \ge q_1(\varepsilon) > 0$; then

$$\left| \sum_{p \le N} \chi\big(f(p)\big) \right| \le \pi(N)\, q^{-\delta}\,, \tag{4}$$

where $\delta = \delta(\varepsilon) > 0$.

The inequality (4) implies asymptotic formulae for the cardinality of the set of quadratic residues, non-residues, primitive roots modulo q among the numbers of the form $p + a$, $p \le N$, for $N \ge q^{1+\varepsilon}$.

§10. One can apply the analytic Dirichlet–Riemann method to the sum S_N. Denoting by $\pi(N; q, l)$ the cardinality of the set of primes of the form $p \equiv l \pmod q$, $p \le N$, we obtain

$$S_N = \sum_{p \le N} \chi(f(p)) = \sum_{l=1}^{q-1} \chi(f(l))\pi(N; q, l) + \Theta,$$

$|\Theta| \le 1$.

Assuming that the extended Riemann hypothesis is correct (that is, all complex zeros of all Dirichlet L-functions lie on the critical straight line) and applying the estimate (2), we obtain:

$$\begin{aligned} \pi(N;\, q, l) &= \frac{\pi(N)}{q-1} + O\big(\sqrt{N}\log(qN)\big); \\ S_N &= O\left(\frac{\pi(N)}{\sqrt{q}}\right) + O\big(q\sqrt{N}\log(qN)\big) \\ &= O\left(\pi(N)\left(\frac{1}{\sqrt{q}} + \frac{q\log^2(qN)}{\sqrt{N}}\right)\right). \end{aligned}$$

From this one sees that the inequality (4) will be valid only for

$$N \ge q^{2+\varepsilon}.$$

Note that if one uses explicit formulae for $\pi(N;\, q, l)$, that is, if one writes $\pi(N;\, q, l)$ as a sum over the zeros of Dirichlet L-series of modulus q, if one applies the extended Riemann hypothesis and the estimate (2), then (4) will be valid for

$$N \ge q^{1+\varepsilon},$$

i.e., it will be an analogue of Vinogradov's 1938 result for linear polynomials $f(x) = x + a$. One intuitively understands that the analytic Dirichlet–Riemann method works only when there appears an "order" in the distribution of primes p, $p \le N$, modulo q, and this happens, at best, only when $N \ge q^{1+\varepsilon}$.

§11. In 1952, I. M. Vinogradov [5] obtained the inequality (4) for

$$N \ge q^{0.75+\varepsilon}.$$

It looked as if there was obtained what could not be obtained. Yu. V. Linnik wrote on this in 1971 (cf. [22; p. 29]): "This estimate is a matter of principle, because by its depth it surpasses that what is given by an immediate application of the extended Riemann hypothesis, and apparently it is a truth more thorough than the hypothesis mentioned above (if the hypothesis is true)."

§ 12. In 1970, the author succeeded in proving the inequality (4) with

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

We shall comment below on how to obtain this result. But still a few words on further development of the subject matter. Estimates of $|S_N|$ of the form (4) worked well only for linear polynomials f, $f(x) = x + a$. In 1978, the author obtained (4) with

$$N \geq q^{0.75+\varepsilon}, \quad f(x) = (x+a)(x+b), \qquad a \not\equiv b \pmod q.$$

This implies, for instance, the following purely arithmetic result: Let $\chi(n)$ be the Legendre symbol modulo q, $ab(a-b) \not\equiv \pmod q$, $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm 1$, and $T(N)$ be the cardinality of the set of primes p not exceeding N and such that

$$\chi(p+a) = \varepsilon_1, \qquad \chi(p+b) = \varepsilon_2,$$

then for $N \geq q^{0.75+\varepsilon}$, $0 < \varepsilon < 0.01$, one has the following asymptotic formula:

$$T(N) = \frac{1}{4}\pi(N) + O\big(Nq^{-0.01\varepsilon^2}\big).$$

§ 13. The following is a basic idea for obtaining the results of §12 (it has been worked out and applied by the author in the papers [8]–[21]). Let us study the double sum W,

$$W = \sum_{x \in \mathbb{X}} \sum_{z \in \mathbb{Y}} \chi(x+y), \tag{5}$$

where X and Y are arbitrary sets of positive integers without repetition, each of them being less than q, and let

$$X = \|\mathbb{X}\|, \qquad Y = \|\mathbb{Y}\|,$$

be the cardinalities of these sets. Further, if

$$X \geq q^{0.5+\varepsilon}, \quad Y \geq q^{\varepsilon}, \qquad \varepsilon > 0,$$

and $\varepsilon > 0$ is arbitrary, then for $|W|$ we have a nontrivial estimate of the form:

$$|W| \leq XYq^{-\delta}, \qquad \delta = \delta(\varepsilon) > 0, \quad q \geq q_1(\varepsilon) > 0.$$

In this way, for any $\mathbb{X}, \mathbb{Y}$, the summands of the sum W oscillate, and one succeeds in "catching" the oscillation.

The estimate of $|W|$ is obtained in the following way. For a natural number k, by applying the Hölder inequality, we find

$$\begin{aligned} |W|^{2k} &\le X^{2k-1} \sum_{x \in \mathbb{X}} \left| \sum_{y \in \mathbb{Y}} \chi(x+y) \right|^{2k} \\ &\le X^{2k-1} \sum_{y_1, \ldots, y_{2k} \in \mathbb{Y}} \sum_{x=1}^{q} \chi\Big((x+y_1)\ldots(x+y_{2k})^{-1}\Big). \end{aligned}$$

One applies (1) to the internal sum over x for those $2k$-tuples $(y_1, \ldots, y_{2k})$ for which (1) is valid. Such $2k$-tuples constitute the bulk. Few of the $2k$-tuples $(y_1, \ldots, y_{2k})$ do not fulfil (1). Then choosing k, $k = k(\varepsilon)$, in an optimum way, one obtains the estimate of $|W|$ mentioned above.

§14. After the general idea of §13, one may ask how to reduce the sum S_N to W. One applies here the sieve method of I. M. Vinogradov that has its origin in the sieve of Eratosthenes, and is analytically realized with the help of the Möbius function. The sieve method of I. M. Vinogradov is well explained in [4–7], and also in the monograph I. M. Vinogradov, Izbrannye trudy. [Selected works.] Izdat. Akad. Nauk SSSR, Moscow, 1952 (p. 221 or 313). In addition to this, one uses a special method elaborated in the author's articles [8–12], allowing to increase the cardinality of the set $\mathbb{X}$ (or of the set $\mathbb{Y}$) if the numbers from $\mathbb{X}$ (from $\mathbb{Y}$) possess certain arithmetic properties. In this way, roughly speaking, one obtains the result for $f(x) = x + a$.

§15. To obtain the result of §12 for an arbitrary polynomial $f(x)$ of degree ≥ 2, one needs the following theorem:

Let $f(x)$ be a polynomial with integer coefficients,

$$f(x) \not\equiv g^m(x) \pmod{q},$$

$a_1, a_2, \ldots, a_k$ be integers such that

$$a_i \not\equiv a_j \pmod{q}, \qquad i \ne j,$$

$f(x)$ be of degree ≥ 2, and let

$$F(x,y) = f(x+a_1 y)\, f(x+a_2 y) \ldots f(x+a_k y). \tag{6}$$

Then one has the estimate

$$\sum_{x=1}^{q} \sum_{y=1}^{q} \chi\big(F(x,y)\big) = O(q). \tag{7}$$

The estimate (7) for "generic" polynomials $F(x,y)$ was obtained by Deligne. For the polynomial $F(x,y)$ from (6), the Deligne theorem fails. However if

$f(x) = (x+a)(x+b)$, then (7) is obtained from (1) (cf. [15; p. 316–317]). In [14], a conditional theorem is proved on estimates of $|S_N|$ for any polynomial $f(x)$ and $N \geq q^{0.75+\varepsilon}$.

§ 16. Along with S_N the author studied the sums

$$T_N = \sum_{n \geq N} \tau_k(n)\chi(n+a), \quad a \not\equiv 0 \pmod{q},$$
$$V_N = \sum_{n \leq N} \tau_k(n)\chi\big((n+a)(n+b)\big), \quad a \not\equiv \pmod{q};$$

here $\tau_k(n)$ means the number of positive-integer solutions $n_1, \ldots, n_k$ of the equation $n_1 \ldots n_k = n$. In [18] and [19] the following estimates have been obtained:

$$|T_N| \leq Nq^{-0.01\varepsilon^2}, \qquad q^2 \geq N \geq q^{0.5+\varepsilon}, \quad q \geq q_1(\varepsilon),$$
$$|V_N| \leq Nq^{-0.01\varepsilon^2}, \qquad q^2 \geq N \geq q^{0.75+\varepsilon}, \quad q \geq q_1(\varepsilon).$$

Papers [20] and [21] have been solving problems connected with the value distribution of the Dirichlet characters on additive sequences, i.e., on sequences of positive integers of the form $x+y$, $x \in \mathbb{X}$, $y \in \mathbb{Y}$. In particular, the following theorem is proved in [21]:

Let $\Psi_1(x)$ and $\Psi_2(y)$ be complex-valued functions such that $|\Psi_1(x)| \leq \Psi_1$, $|\Psi(y)| \leq \Psi_2$, $0 < \varepsilon < 0.01$, $q \geq q_1(\varepsilon)$,

$$X \geq q^{\varepsilon}, \quad \sqrt{XY} \geq q^{0.5+\varepsilon};$$

then one has the following estimate:

$$\left| \sum_{x \leq X} \sum_{y \leq Y} \Psi_1(x)\Psi_2(y)\chi(x+y+a) \right| \leq XY\Psi_1\Psi_2 q^{-0.01\varepsilon^2}.$$

In [12], [16], [17], the author has studied sums similar to S_N, with $f(x) = x+a$ or $f(x) = (x+a)(x+b)$, over primes p belonging to an arithmetic progression, i.e., $p \equiv l\ (k)$, $(l,k) = 1$; the difference k of the progression was permitted to grow exponentially depending on the growth of the modulus q of the character. In this way, sparse sequences of primes were obtained, at which it was possible to study how the values $\chi(p+a)$, $\chi\big((p+a)(p+b)\big)$ are distributed.

§ 17. In recent years the author proved new theorems on estimates for $|S_N|$, $|T_N|$, $|V_n|$. In particular, one has the following propositions:

1. If $f(x) = (x+a)^{\alpha}(x+b)^{\beta}$, where α and β are positive integers such that at least one of them is not divisible by m, $a \not\equiv b \pmod{q}$, then

$$|S_N| \leq Nq^{-0.01\varepsilon}, \quad q^2 \geq N \geq q^{0.75+\varepsilon}, \quad 0 < \varepsilon < 0.01, \quad q \geq q_1(\varepsilon) > 0.$$

This estimate implies, for instance, an asymptotic formula for the number of primes p, $p \le N$, such that the numbers $(p+a)^\alpha$ and $(p+b)^\beta$, $ab(a-b) \not\equiv 0 \pmod q$, at the same time, primitive roots modulo q.

2. Let $0 < |a| \le \sqrt{q}$, $0 < \varepsilon < 0.01$, $q \ge q_1(\varepsilon) > 0$, $N \ge q^{\frac{1}{2} - \frac{1}{2(k+1)} + \varepsilon}$; then we have the following estimate:

$$|T_N| \le N q^{-0.01\varepsilon^2}.$$

If $k = 2$, then one obtains a nontrivial estimate of $|T_N|$ for $N \ge q^{\frac{1}{3}+\varepsilon}$; earlier, in [18], a similar estimate was available only for $N \ge q^{\frac{1}{2}+\varepsilon}$. Analogous strengthenings are also obtained for K_N,

$$K_N = \sum_{n \le N} \tau_k(n) \chi\big((n+q)^\alpha (n+b)^\beta\big), \qquad a \not\equiv b \pmod q.$$

§18. Problems.

1. Prove (7) for polynomials $F(x,y)$ of the form (6); in this way, the result from [14] becomes unconditional.
2. Prove (4) for $f(x) = x + a$, $N \ge q^\delta$, $\delta < \frac{1}{2}$.
3. Prove (4) for $f(x) = (x+a)(x+b)$,
4. Learn how to estimate, in a nontrivial way, $|S_N|$ for $f(x) = x$.

REFERENCES

[1] VINOGRADOV, I. M.: *Sur la distribution des residues et des nonresidues des puisances*, J. Phys. Math. Soc. Perm Univ. **1** (1918), 94–98.

[2] VINOGRADOV, I. M.: *On the distribution of quadratic residues and non-residues*, J. Phys. Math. Soc. Perm Univ. **2** (1919), 1–16. (In Russian)

[3] VINOGRADOV, I. M.: *New theorems on the distribution of quadratic residues*, Dokl. Akad. Nauk SSSR **1** (1934), 289–290, French summary. (In Russian)

[4] VINOGRADOV, I. M.: *The distribution of quadratic residues and non-residues of the form $p+k$ to a prime modulus*, Matemat. sb. **3** (1938), 311–320, English summary. (In Russian)

[5] VINOGRADOV, I. M.: *New approach to the estimation of sums of values $\chi(p+k)$*, Izv. Akad. Nauk SSSR, Ser. Mat. **16** (1952), 197–210. (In Russian)

[6] VINOGRADOV, I. M.: *An improvement of estimation of sums of values $\chi(p+k)$*, Izv. Akad. Nauk SSSR, Ser. Mat. **17** (1953), 285–290. (In Russian)

[7] VINOGRADOV, I. M.: *An estimate for a certain sum extended over the primes of an arithmetic progression*, Izv. Akad. Nauk SSSR, Ser. Mat. **30** (1966), 481–496. (In Russian)

[8] KARATSUBA, A. A.: *Sums of characters and primitive roots in finite fields*, Sov. Math., Dokl. **9** (1968), 755–757; translation from Dokl. Akad. Nauk SSSR **180** (1968), 1287–1289. (In Englisch, in Russian)

[9] KARATSUBA, A. A.: *On sums of characters with primes*, Sov. Math., Dokl. **11**, 135–137 (1970); translation from Dokl. Akad. Nauk SSSR **190** (1970), 517–518. (In Englisch, in Russian)

[10] KARATSUBA, A. A.: *On estimates of character sums*, Izv. Akad. Nauk SSSR, Ser. Mat. **34** (1970), 20–30. (In Russian)

[11] KARATSUBA, A. A.: *Sums of characters with prime numbers*, Izv. Akad. Nauk SSSR, Ser. Mat. **34** (1970), 299–321. (In Russian)

[12] KARATSUBA, A. A.: *Sums of characters with primes that belong to an arithmetic progression*, Izv. Akad. Nauk SSSR, Ser. Mat. **35** (1971), 469–484. (In Russian)

[13] KARATSUBA, A. A.: *On the distribution of values of nonprincipal characters*, Proc. Steklov Inst. Math. **142** (1979), 165–174; translation from Trudy Mat. Inst. Steklov **142** (1976), 156–164. (In Englisch, in Russian)

[14] KARATSUBA, A. A.: *Distribution of the values of Legendre symbols in polynomials with prime numbers*, Sov. Math., Dokl. **19** (1978), 61–63; translation from Dokl. Akad. Nauk SSSR **238** (1978), 524–526. (In Englisch, in Russian)

[15] KARATSUBA, A. A.: *Sums of Legendre symbols of quadratic polynomials with prime numbers*, Izv. Akad. Nauk SSSR, Ser. Mat. **42** (1978), 315–324. (In Russian)

[16] KARATSUBA, A. A.: *Quadratic residues and nonresidues in sparse sequences*, Sov. Math., Dokl. **30** (1984), 767–768; translation from Dokl. Akad. Nauk SSSR **279** (1984), 1044–1046. (In English, in Russian)

[17] KARATSUBA, A. A.: *Distribution of pairs of quadratic residues and nonresidues of special form*, Izv. Akad. Nauk SSSR, Ser. Mat. **51** (1987), 994–1009. (In Russian)

[18] KARATSUBA, A. A.: *On a certain arithmetic sum*, Sov. Math., Dokl. **12** (1971), 1172–1174; translation from Dokl. Akad. Nauk SSSR **199** (1971), 770–772. (In Englisch, in Russian)

[19] KARATSUBA, A. A.: *Asymptotic of an arithmetical sum*, Mat. zametki **24** (1978), 737–740. (In Russian)

[20] KARATSUBA, A. A.: *Distribution of power residues and nonresidues in additive sequences*, Sov. Math., Dokl. **12** (1971), 235–236; translation from Dokl. Akad. Nauk SSSR **196** (1970), 759–760. (In Englisch, in Russian)

[21] KARATSUBA, A. A.: *The distribution of values of Dirichlet characters on additive sequences*, Sov. Math., Dokl. **44** (1992), 145–148; translation from Dokl. Akad. Nauk SSSR **319** (1991), 543–544. (In English, in Russian)

[22] LINNIK, Yu. V.: *Recent works of I. M. Vinogradov*, Proc. Steklov Inst. Math. **132** (1973), 25–28 (1975); translation from Trudy Mat. Inst. Steklov **132** (1973), 27–29. (In Englisch, in Russian)

[23] LIDL, R.—NIEDERREITER, G.: *Finite Fields*, Addison–Wesley, Reading, Mass., 1983; Mir, Moskva, 1988.

Received December 20, 1999

Steklov Mathematical Institute
Gubkina str. 8
117966 Moscow, GSP–1
RUSSIA

E-mail: karatsuba@mi.ras.ru