[3] Y. Dupain, *Intervalles à restes majorés pour la suite (nα)*, Acta Math. Acad. Sci. Hungar. 29 (1977), pp. 289–303.

[4] — *Intervalles à restes majores pour la suite (nα)*, Bull. Soc. Math. France (to appear).

[5] H. Furstenberg, H. Keynes, L. Shapiro, *Prime flows in topological dynamics*, Israel J. Math. 14 (1973), pp. 26–38.

[6] G. Halász, *Remarks on the remainder in Birkhoff's ergodic theorem*, Acta Math. Acad. Sci. Hungar. 27 (1976), pp. 389–396.

[7] E. Hecke, *Über analytische Functionen und die Verteilung von Zahlen mod Eins*, Abh. Math. Sem. Hamburg 1 (1922), pp. 54–76.

[8] H. Kesten, *On a conjecture of Erdös and Szüsz related to uniform distribution mod 1*, Acta Arith. 12 (1966), pp. 193–212.

[9] M. R. Herman, *Conjugasion C^∞ des difféomorphismes du cercle dont le nombre de rotation satisfait à une condition arithmétique*, C. R. Acad. Sci., Paris, 282 (1976), pp. A503–A506.

[10] — *Sur la conjugasion différentiable des difféomorphismes du cercle à des rotations*, Thèses, Orsay, CNRS, No. A.O. 12. 451.

[11] J. Lesca, *Sur la repartition modulo 1 des suites*, Seminaire Delange–Pisot–Poiton (1966–67), f.1, n.2.

[12] — *Sur la repartition modulo 1 de la suite nα*, Acta Arith. 20 (1972), pp. 345–352.

[13] A. Ostrowski, *Bemerkungen zur Theorie der diophantischen Approximationen*, Abh. Math. Sem. Hamburg 1 (1922), pp. 77–98.

[14] K. Petersen, *On a series of cosecants related to a problem in ergodic theory*, Comp. Math. 26 (3) (1973), pp. 313–317.

[15] V. T. Sós, *On the theory of diophantine approximation I*, Acta Math. Acad. Sci. Hungar. 8 (1957), pp. 461–472.

[16] — *On the distribution of the sequence {nα}*, Tagungsbericht Math. Inst., Oberwolfach, 28 (1972).

[17] — *On the discrepancy of the sequence {nα}*, Coll. Math. Soc. J. Bolyai, Vol. 13, pp. 359–367, 1976.

[18] — *On the theory of diophantine approximation II*, Acta Math. Acad. Sci. Hungar. 9 (1958), pp. 229–241.

U.E.R. DE MATHÉMATIQUES ET INFORMATIQUE
UNIVERSITÉ DE BORDEAUX I
Talence, France

EÖTVÖS LORÁND UNIVERSITY
DEPARTMENT OF ANALYSIS I
Budapest, Hungary

Received on 15. 2. 1978 (1044)

ACTA ARITHMETICA
XXXVII (1980)

An exponential polynomial formed with the Legendre symbol

by

HUGH L. MONTGOMERY (Ann Arbor, Mich.)

Dedicated to the memory of Paul Turán

We investigate the behavior of the sum

$$S(\alpha) = S_p(\alpha) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e(n\alpha), \tag{1}$$

which is a particular example of an exponential polynomial of the sort

$$S(\alpha, \varepsilon) = \sum_{n=1}^{N} \varepsilon_n (n\alpha) \tag{2}$$

with $\varepsilon_n = \pm 1$. Among such polynomials, $S(\alpha)$ has the unusual property that

$$|S(a/p)| = \sqrt{p} \quad (1 \leqslant a \leqslant p-1), \tag{3}$$

and $S(0) = 0$. It is difficult to exhibit a choice of ε for which $|S(\alpha, \varepsilon)| \leqslant C\sqrt{N}$ for all α. The example known was found by H. S. Shapiro [5] and W. Rudin [4]; a nice account of this and related problems was given by Littlewood [3], pp. 25–32. In view of (3), we ask whether the sum $S(\alpha)$ also satisfies the bound $S(\alpha) \ll \sqrt{p}$. Indeed, from Bernstein's inequality it follows that if $K > \frac{\pi}{2} N$ then

$$\max_\alpha |S(\alpha, \varepsilon)| \leqslant \left(1 - \frac{\pi N}{2K}\right)^{-1} \max_a |S(a/K, \varepsilon)|;$$

thus the points a/p are nearly dense enough for us to deduce from (3) that $S(\alpha) \ll p^{1/2}$. Hence it is surprising that this estimate is false for *all* large primes p.

THEOREM. *For $p > 2$, $S(\alpha) \ll p^{1/2}\log p$, and for all large p,*

$$\max_\alpha |S(\alpha)| > \frac{2}{\pi} p^{1/2} \log\log p. \tag{4}$$

Later we discuss the distribution of values of $S(\alpha)$, and we conjecture that there is a constant C so that

$$\max_{\alpha}|S(\alpha)| \leqslant Cp^{1/2}\log\log p; \tag{5}$$

thus our lower bound (4) is expected to be sharp.

The proof of our theorem is based on the following two lemmas.

Lemma 1. *Let χ be a primitive character* (mod q), $q > 1$. *Then*

$$\sum_{n=0}^{q-1}\chi(n)e(n\alpha) = \tau(\chi)q^{-1}e(\tfrac{1}{2}q\alpha)(\sin\pi q\alpha)T(\alpha,\overline{\chi}), \tag{6}$$

where $\tau(\chi)$ *is the Gauss sum*

$$\tau(\chi) = \sum_{n=1}^{q}\chi(n)e(n/q), \tag{7}$$

and

$$T(\alpha,\chi) = \sum_{a=1}^{q}\chi(a)\cot\pi(\alpha - a/q). \tag{8}$$

Proof. Since χ is primitive, we have

$$\chi(n) = \tau(\chi)^{-1}\sum_{a=1}^{q}\overline{\chi}(a)e(an/q) \tag{9}$$

for all n. Thus the left hand side of (6) is

$$= \tau(\overline{\chi})^{-1}\sum_{a=1}^{q}\overline{\chi}(a)\sum_{n=0}^{q-1}e\big(n(\alpha - a/q)\big)$$

$$= \tau(\overline{\chi})^{-1}\big(1-e(q\alpha)\big)\sum_{a=1}^{q}\overline{\chi}(a)\big(1-e(\alpha + a/q)\big)^{-1}.$$

We write $-a$ for a, and recall that $\tau(\chi)\tau(\overline{\chi}) = \chi(-1)q$ for primitive χ; thus the above is

$$= \tau(\chi)q^{-1}\big(1-e(q\alpha)\big)\sum_{a=1}^{q}\overline{\chi}(a)\big(1-e(\alpha - a/q)\big)^{-1}$$

$$= \tau(\chi)q^{-1}e(\tfrac{1}{2}q\alpha)(\sin q\alpha)\sum_{a=1}^{q}\overline{\chi}(a)e\big(-\tfrac{1}{2}(\alpha - a/q)\big)\big(\sin\pi(\alpha - a/q)\big)^{-1}.$$

We now write $e\big(-\tfrac{1}{2}(\alpha - a/q)\big) = \cos\pi(\alpha - a/q) - i\sin\pi(\alpha - a/q)$, and recall that $\sum_{a=1}^{q}\overline{\chi}(a) = 0$ to see that the sum above is $= T(\alpha,\overline{\chi})$; this gives (6).

On letting α tend to a/p, we see that (6) includes the familiar relation

$$\sum_{n=0}^{q-1}\chi(n)e(an/q) = \tau(\chi)\overline{\chi}(a).$$

In fact this is (9) with $\overline{\chi}$ replaced by χ. Since $|\tau(\chi)| = q^{1/2}$ for primitive χ we obtain (3) by taking $\chi(n) = \left(\frac{n}{p}\right)$. By the partial fraction formula for $\cot\pi z$ we see that

$$\sum_{a=1}^{q}\overline{\chi}(a)\cot\pi(\alpha - a/q) = \frac{q}{\pi}\sum_{-\infty}^{+\infty}\frac{\overline{\chi}(k)}{q\alpha - k},$$

where the sum over k is to be interpreted as $\lim_{K\to\infty}\sum_{-K}^{K}$. Thus (6) can be considered to be a special case of the functional equation for a generalized zeta function.

Lemma 2. *For $k \geqslant 1$ let $a_1, \ldots, a_k$ be integers, distinct* (mod p), *and put* $f(x) = \prod(x - a_i)$. *Then*

$$\left|\sum_{n=1}^{p}\left(\frac{f(n)}{p}\right)\right| \leqslant (k-1)p^{1/2}.$$

This is a consequence of Weil's Riemann Hypothesis for the zeta function of a curve over a finite field; see Weil [6], [7]. The derivation of the particular bound above is given by Burgess ([1]; § 2).

To obtain the theorem, we put $\chi(n) = \left(\frac{n}{p}\right)$ in Lemma 1. Since then $|\tau(\chi)| = p^{1/2}$, the first assertion is immediate on noting that

$$|\tau(\chi,\alpha)| \leqslant \sum_{a=1}^{p-1}|\cot\pi(\alpha - a/p)| \leqslant \frac{1}{\pi}\sum_{a=1}^{p-1}\|\alpha - a/p\|^{-1} \ll p(\|p\alpha\|^{-1} + \log p).$$

Again from (6), the second assertion is a consequence of the inequality

$$\max_{n}\left|T\left(\frac{2n+1}{2p}\right)\right| \geqslant \frac{2}{\pi}p\log\log p, \tag{10}$$

where $T(\alpha) = T\left(\left(\frac{*}{p}\right),\alpha\right)$. If $\left(\frac{h}{p}\right) = 1$ for $h = n, n-1, \ldots, n-H$, and $\left(\frac{h}{p}\right) = -1$ for $h = n+1, n+2, \ldots, n+H$, then we may expect that

$T\left(\frac{2n+1}{2p}\right)$ is approximately

$$\sum_{n-H}^{n+H}\left|\cot\pi\left(\frac{2n-2h+1}{2p}\right)\right| \sim \frac{2}{\pi}p\log H.$$

With this in mind we put

$$W(n) = \prod_{h=1}^{H}\left(1-\left(\frac{n+h}{p}\right)\right)\prod_{h=0}^{H}\left(1+\left(\frac{n-h}{p}\right)\right), \tag{11}$$

and compute the size of the weighted sum

$$\sum_{n=1}^{p} T\left(\frac{2n+1}{p}\right)W(n). \tag{12}$$

On mutliplying out the product (11), we see that

$$W(n) = 1+\sum_{f}\pm\left(\frac{f(n)}{p}\right),$$

where f runs through $2^{2H+1}-1$ polynomials of the sort considered in Lemma 2. Hence by this lemma,

$$\sum_{n=1}^{p} W(n) = p+O(H2^{2H}p^{1/2}). \tag{13}$$

Similarly,

$$\sum_{n=1}^{p} W(n)\left(\frac{n-a}{p}\right) = c(a)p+O(H2^{2H}p^{1/2})$$

where $c(a) = 1$ if $0\leqslant a\leqslant H$, $c(a) = 0$ if $H<a<p-H$, and $c(a) = -1$ if $p-H\leqslant a<p$. Hence the expression (12) is

$$= \frac{4p}{\pi}\sum_{a=1}^{H}\frac{1}{2a-1}+O(p/H)+O(H^2/p)$$

$$= \frac{2}{\pi}p(\log H+C)+O(p/H)+O(H^2/p),$$

where $C = 2\log 2+\gamma = 1.9635\ldots$ Taking $H = \frac{1}{4}\log p$, we find that

$$\sum_{n=1}^{p} W(n)T\left(\frac{2n+1}{2p}\right) = \frac{2}{\pi}p^2(\log\log p+\gamma)+O(p^2/\log p).$$

But $W(n)$ is non-negative, so

$$\max_n T\left(\frac{2n+1}{2p}\right) \geqslant \left(\sum_n W(n)T\left(\frac{2n+1}{2p}\right)\right)\left(\sum_n W(n)\right)^{-1}$$

$$= \frac{2}{\pi}p(\log\log p+\gamma)\left(1+O\left(\frac{1}{\log p}\right)\right)$$

$$> \frac{2}{\pi}p\log\log p$$

for large p.

By the Pólya–Vinogradov inequality we see that if $p\equiv 3 \pmod 4$ then

$$T\left(\frac{1}{2p}\right) = -\frac{2}{\pi}pL\left(1,\left(\frac{*}{p}\right)\right)+O(p).$$

Joshi [2] has shown that there are infinitely many primes $p\equiv 3 \pmod 4$ for which $L\left(1,\left(\frac{*}{p}\right)\right) > (e^{\gamma}-\varepsilon)\log\log p$. Thus for infinitely many p,

$$\max_{\alpha}|S(\alpha)| \geqslant \left(\frac{2}{\pi}e^{\gamma}-\varepsilon\right)p^{1/2}\log\log p.$$

It seems likely that for $N>(\log p)^2$,

$$\sum_{r=m+1}^{m+N}\left(\frac{n}{p}\right) \ll N\left(\log\frac{2N^{1/2}}{\log p}\right)^{-2};$$

this would give $T(\alpha) \ll p(\|p\alpha\|^{-1}+\log\log p)$, and consequently (5).

We have seen that the behavior of $S(\alpha)$ is atypical when compared with that of $S(\alpha, \varepsilon)$ for most ε. However, it can be shown that the distribution of the values of $S(\alpha)/\tau\left(\left(\frac{*}{p}\right)\right)$ is approaching a limiting distribution which is the same as the limit of the distribution of the values of $S^*(\alpha, \varepsilon)$ for almost all ε, where

$$S^*(\alpha, \varepsilon) = p^{-1}e(\tfrac{1}{2}p\alpha)\sin\pi p\alpha\sum_{a=1}^{p}\varepsilon_a\cot\pi(\alpha-a/p).$$

References

[1] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika 4 (1957), pp. 106–112.

[2] P. T. Joshi, *The size of $L(1,\chi)$ for real nonprincipal residue characters χ with prime modulus*, J. Number Theory 2 (1970), pp. 58–73.

[3] J. E. Littlewood, *Some problems in real and complex analysis*, Heath (Lexington), 1968.
[4] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. 10 (1959), pp. 855–859.
[5] H. S. Shapiro, Masters thesis, MIT, 1957.
[6] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Math. et Sci., No. 1041 (1945).
[7] — *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), pp. 497–508.

UNIVERSITY OF MICHIGAN
Ann Arbor, Michigan, U.S.A.

Received on 18. 2. 1978 (1046)

ACTA ARITHMETICA
XXXVII (1980)

Об интегралах, содержащих остаточный член проблемы делителей

А. Ф. Лаврик, М. И. Исраилов, Ж. Ёдгоров (Ташкент)

Памяти П. Турана посвящается

Пусть $\tau_k(n)$ обозначает число решений уравнения $n = m_1 \dots m_k$ в целых положительных числах $m_1, \dots, m_k$. Положим

$$\sum_{n\leqslant x} \tau_k(n) = xP_k(\log x) + \Delta_k(x), \tag{1}$$

где $xP_k(\log x)$ — главный член роста суммы (вычет в точке $s = 1$ функции $\zeta^k(s)x^s/s$, ζ — дзета-функция Римана).

В работе [1] были выписаны коэффициенты $a_j^{(k)}$ полинома:

$$P_k(\log x) = a_{k-1}^{(k)}\log^{k-1}x + \dots + a_1^{(k)}\log x + a_0^{(k)}, \tag{2}$$

которые выражаются через $\gamma_0, \gamma_1, \dots, \gamma_k$ определяемые соотношением:

$$\gamma_n = \frac{(-1)^n}{n!} \lim_{M\to\infty} \left[\sum_{1\leqslant m\leqslant M} \frac{\log^n m}{m} - \frac{\log^{n+1} M}{n+1} \right]. \tag{3}$$

Опираясь на этот результат здесь в отношении остаточного члена $\Delta_k(x)$ доказывается следующая

Теорема. *Для любого целого числа $k \geqslant 1$ имеем*

$$\int_1^\infty \frac{\Delta_k(u)}{u^2}\, du = a_0^{(k+1)} - \sum_{m=0}^{k-1} m!\,\gamma_m a_m^{(k)}. \tag{4}$$

Вывод теоремы основывается на двух леммах.

Лемма 1. *Для любого целого $n \geqslant 0$ и любого вещественного $x \geqslant 1$ имеют место следующие равенства*

$$\sum_{1\leqslant m\leqslant x} \frac{\log^n m}{m} = \frac{\log^{n+1} x}{n+1} + (-1)^n n!\,\gamma_n + O\left(\frac{\log^n x}{x}\right), \tag{5}$$

$$\sum_{1\leqslant m\leqslant x} \frac{\log^n (x/m)}{m} = \frac{\log^{n+1} x}{n+1} + \sum_{k=0}^{n} k!\,C_n^k \gamma_k \log^{n-k} x + O\left(\frac{\log^n x}{x}\right). \tag{6}$$