Composition Mathematica

Imre Z. Ruzsa
Andrzej Schinzel

An application of Kloosterman sums

Compositio Mathematica, tome 96, nº 3 (1995), p. 323-330
<http://www.numdam.org/item?id=CM_1995__96_3_323_0>

Compositio Mathematica **96**: 323–330, 1995.

An application of Kloosterman sums

IMRE Z. RUZSA*[1] and ANDRZEJ SCHINZEL[2]
[1] *Mathematical Institute of the Hungarian Academy of Sciences, Budapest, Pf. 127, H-1364 Hungary*
[2] *Instytut Matematyczny PAN, ul. Śniadeckich 8, Skr. poczt. 137, 00-950 Warszawa, Poland*

Received: 16 December 1993; accepted in final form 11 May 1994

To the memory of Professor A. V. Malyshev.

Let n be a positive integer

$$A_n = \{a : 1 \leqslant a \leqslant n,\ (a,\ n) = 1\},$$

and for $a \in A_n$ let $\bar{a}$ denote the unique element of A_n satisfying $a\bar{a} \equiv 1 \pmod n$. For n odd, $\varepsilon = 0$ or 1, $\delta = \pm 1$ put

$$L_n^\varepsilon = \{a \in A_n : a - \bar{a} \equiv \varepsilon \pmod 2\},$$

$$L_n^{\varepsilon,\delta} = \left\{a \in A_n : a - \bar{a} \equiv \varepsilon \pmod 2,\ \left(\frac{a}{n}\right) = \delta\right\}.$$

Zhang Wenpeng [5] recently conjectured that for every odd n and $\eta > 0$

$$\#L_n^1 = \tfrac{1}{2}\phi(n) + O(n^{1/2+\eta})$$

and proved it, even in a somewhat stronger form for n being a prime power or a product of two primes.

On the other hand, G. Terjanian [4] conjectured that $L_p^{\varepsilon,\delta} \neq \emptyset$ for every prime $p > 29$ and every choice of ε and δ. This conjecture has been proved by Chaładus [1] by applying Nagell's bound for the least quandratic nonresidue modulo p.

We prove the following theorem, which confirms Zhang's conjecture, improves his error term for n being a prime power, and improves Chaładus's theorem except for finitely many primes.

THEOREM 1. *For every choice of* $\varepsilon = 0,\ 1$ *and* $\delta = \pm 1$ *we have*

$$\#L_n^{\varepsilon,\delta} = \frac{\phi(n)}{4} c_{n,\delta} + O(2^{\nu(n)}\sqrt{n}(\log n)^2), \tag{1}$$

* Supported by Hungarian National Foundation for Scientific Research, Grant No. 1901.

where

$$c_{n,\delta} = \begin{cases} 1+\delta & \text{if } n \text{ is a perfect square,} \\ 1 & \text{otherwise.} \end{cases}$$

and $\nu(n)$ is the number of distinct prime factors of n.

Consider a positive integer n, not necessarily odd, a positive integer m coprime to n, $0 \leqslant j,\ k < m$, an odd divisor r of n, $\delta = \pm 1$ and put

$$S_n^m(j,\ k,\ r,\ \delta) = \#\left\{a \in A_n : a \equiv j \pmod m,\ \bar{a} \equiv k \pmod m,\ \left(\frac{a}{r}\right) = \delta\right\}.$$

We shall deduce Theorem 1 from the following estimate of this quantity.

THEOREM 2. *For any choice of $m < n$, coprime to n, $0 \leqslant j,\ k < m$, odd r dividing n and $\delta = \pm 1$ we have*

$$S_n^m(j,\ k,\ r,\ \delta) = \frac{\phi(n)}{2m^2} c_{r,\delta} + O(2^{\nu(n)}\sqrt{n}(\log n)^2),$$

where the constant in the O symbol is absolute and effective.

To obtain Theorem 1 from Theorem 2 we only need to observe that

$$\#L_n^{0,\delta} = S_n^2(0,\ 0,\ n,\ \delta) + S_n^2(1,\ 1,\ n,\ \delta),$$
$$\#L_n^{1,\delta} = S_n^2(0,\ 1,\ n,\ \delta) + S_n^2(1,\ 0,\ n,\ \delta).$$

The proof of Theorem 2 is based on four lemmas.

LEMMA 1. *If r is an odd divisor of n, we have*

$$\left|\sum_{u\in A_n} \left(\frac{u}{r}\right) e\left(\frac{uv}{n}\right)\right| \leqslant \sqrt{n(v,\ n)},$$

where $e(t) = \exp(2\pi i t)$.

Proof. $\left(\frac{u}{r}\right)$ is a character mod n, whose conductor f is equal to the squarefree kernel of r. Hence by a known formula (see [2], Chapter IV, Sect. 20, assertion IV)

$$\left|\sum_{u\in A_n} \left(\frac{u}{r}\right) e\left(\frac{uv}{n}\right)\right| = \begin{cases} \frac{\phi(n)}{\phi(n/(v,\ n))} \left|\mu\left(\frac{n}{(v,\ n)}\right)\right| \sqrt{f} & \text{if } f \left| \frac{n}{(v,\ n)}\right., \\ 0 & \text{otherwise.} \end{cases}$$

Since

$$\phi\left(\frac{n}{(v,\ n)}\right) \geqslant \frac{\phi(n)}{(v,\ n)},$$

we obtain

$$\left|\sum_{u\in A_n}\left(\frac{u}{r}\right)e\left(\frac{uv}{n}\right)\right| \leqslant \begin{cases} \sqrt{f}(v, n) & \text{if } f(v, n)|n, \\ 0 & \text{otherwise,}\end{cases}$$

which gives the lemma. ∎

LEMMA 2. *For all integers v, w and an odd integer r dividing n*

$$\left|\sum_{u\in A_n}\left(\frac{u}{r}\right)e\left(\frac{uv+\bar{u}w}{n}\right)\right| \leqslant \sqrt{2n2^{\nu}}\sqrt{(v, w, n)}, \tag{2}$$

where ν is the number of distinct prime factors of n.

Proof. This is a slight improvement of a result of Malyshev [3], where instead of the last factor $\min\{\sqrt{(v, n)}, \sqrt{(w, n)}\}$ is obtained. We indicate only the necessary changes to Malyshev's proof to obtain (2).

We use $K_r(v, w, n)$ to denote the sum in the left side of (2). For prime-powers Malyshev shows

$$|K_r(v, w, p^t)| \leqslant C_p p^{t/2}(v, p^t)^{1/2},$$

where $C_p = 2$ for odd primes and $C_2 = 2\sqrt{2}$. By symmetry we also have

$$|K_r(v, w, p^t)| \leqslant C_p p^{t/2}(w, p^t)^{1/2},$$

and, taking into account that

$$\min\{(v, p^t), (w, p^t)\} = (v, w, p^t),$$

we conclude that

$$|K_r(v, w, p^t)| \leqslant C_p p^{t/2}(v, w, p^t)^{1/2}. \tag{3}$$

To treat the case of composite numbers Malyshev establishes the composition rule

$$K_r(v, w, n) = \pm\prod K_{p_i^{s_i}}(v, w_i, p_i^{t_i}), \tag{4}$$

where

$$n = \prod p_i^{t_i}, \quad r = \prod p_i^{s_i}$$

and the numbers w_i satisfy

$$w \equiv \sum w_i(n/p_i^{t_i})^2 \pmod n.$$

This implies that $(v,\ w_i,\ p_i^{t_i}) = (v,\ w,\ p_i^{t_i})$ and hence

$$\prod (v,\ w_i,\ p_i^{t_i}) = (v,\ w,\ n).$$

Consequently on substituting (3) into (4) we obtain

$$|K_r(v,\ w,\ n)| \leqslant \sqrt{n}\sqrt{v,\ w,\ n)}\prod_{p|n} C_p,$$

and (2) follows by noting that $\Pi C_p \leqslant \sqrt{2}\cdot 2^{\nu}$. ∎

LEMMA 3. *For any integer $n \geqslant 2$ we have*

$$\sum_{v=1}^{n-1} \frac{\sqrt{(v,\ n)}}{v} \ll 2^{\nu}\log n,$$

where ν is the number of distinct prime divisors of n.

Proof.

$$\sum_{v=1}^{n-1} \frac{\sqrt{(v,\ n)}}{v} \leqslant \sum_{d|n}\sum_{j=1}^{[n/d]} \frac{\sqrt{d}}{dj} \leqslant \sum_{d|n} d^{-1/2}\sum_{j=1}^{n} 1/j.$$

Here the second sum is $O(\log n)$. We estimate the first sum as follows:

$$\sum_{d|n} d^{-1/2} \leqslant \prod_{p|n}\sum_{i=0}^{\infty} p^{-i/2} = \prod_{p|n}\frac{1}{1-p^{-1/2}} \ll 2^{\nu},$$

since each term is at most 2, except possibly those corresponding to $p = 2$ and $p = 3$. ∎

LEMMA 4. *For any integer $n \geqslant 2$ we have*

$$\sum_{v=1}^{n-1}\sum_{w=1}^{n-1} \frac{\sqrt{(v,\ w,\ n)}}{vw} \ll (\log n)^2.$$

Proof.

$$\sum_{v=1}^{n-1}\sum_{w=1}^{n-1} \frac{\sqrt{(v,\ w,\ n)}}{vw} \leqslant \sum_{d|n}\sum_{i=1}^{[n/d]}\sum_{j=1}^{[n/d]} \frac{\sqrt{d}}{(di)(dj)} \leqslant \sum_{d|n} d^{-3/2}\sum_{i=1}^{n} 1/i\sum_{j=1}^{n} 1/j.$$

Here the first sum is bounded from above by the convergent sum $\Sigma_{k=1}^{\infty} k^{-3/2}$, and the second and third sum is $O(\log n)$. ∎

Proof of Theorem 2. For $0 \leqslant j < m,\ 0 \leqslant u < n$ we define $\phi_j(u)$ as

$$\phi_j(u) = \begin{cases} 1 & \text{if } u \equiv j \pmod{m}, \\ 0 & \text{otherwise} \end{cases}$$

and extend it periodically with period n. Clearly we have

$$S = S_n^m(j,\, k,\, r,\, \delta) = \frac{1}{2} \sum_{u \in A_n} \phi_j(u)\phi_k(\bar{u}) \left(1 + \delta\left(\frac{u}{r}\right)\right). \tag{5}$$

We develop ϕ_j into a trigonometric series:

$$\phi_j(u) = \sum_{v=0}^{n-1} \alpha_{jv} e\left(\frac{uv}{n}\right). \tag{6}$$

A substitution of expansion (6) into (5) yields

$$\begin{aligned} S &= \frac{1}{2} \sum_{v,w=0}^{n-1} \alpha_{jv}\alpha_{kw} \sum_{u \in A_n} e\left(\frac{uv + \bar{u}w}{n}\right)\left(1 + \delta\left(\frac{u}{r}\right)\right) \\ &= \frac{1}{2} \sum_{v,w=0}^{n-1} \alpha_{jv}\alpha_{kw} T_{vw}. \end{aligned} \tag{7}$$

To estimate T_{vw} we distinguish four cases.

(i) If $v = w = 0$, then clearly $T_{vw} = \phi(n)c_{r,\delta}$.

(ii) If $v \neq 0,\ w = 0$, then we have

$$T_{vw} = \sum_{u=1}^{n-1} e\left(\frac{uv}{n}\right)\left(1 + \delta\left(\frac{u}{r}\right)\right).$$

Applying Lemma 1 twice we obtain

$$|T_{vw}| \leqslant 2\sqrt{n(v,\, n)}. \tag{8}$$

(iii) If $v = 0,\ w \neq 0$, then by symmetry

$$|T_{vw}| \leqslant 2\sqrt{n(w,\, n)}. \tag{9}$$

(iv) If $v \neq 0$ and $w \neq 0$, then by Lemma 2

$$|T_{vw}| \leqslant 2^{\nu}(2n(v,w,\,n))^{1/2}. \tag{10}$$

Substituting these estimates into (7) we obtain

$$S = \frac{\phi(n)}{2} c_{r,\delta}\alpha_{j0}\alpha_{k0} + R, \tag{11}$$

where

$$\begin{aligned}|R| \leqslant\; & 2\sqrt{n}\left(\sum_{v=1}^{n-1}|\alpha_{jv}\alpha_{k0}|\sqrt{(v,\,n)} + \sum_{w=1}^{n-1}|\alpha_{j0}\alpha_{kw}|\sqrt{(w,\,n)}\right.\\ & \left. +2^{\nu}\sum_{v=1}^{n-1}\sum_{w=1}^{n-1}|\alpha_{jv}\alpha_{kw}|\sqrt{(v,\,w,\,n)}\right).\end{aligned} \tag{12}$$

The coefficients can be determined from an inversion formula:

$$\begin{aligned}\alpha_{jv} &= \frac{1}{n}\sum_{u=0}^{n-1}\phi_j(u)e\left(-\frac{vu}{n}\right)\\ &= \frac{1}{n}\sum_{l=0}^{L}e\left(-\frac{v}{n}(j+lm)\right), \quad L = \left[\frac{n-1-j}{m}\right].\end{aligned} \tag{13}$$

In particular,

$$\alpha_{j0} = \frac{1}{n}\left[\frac{n-1-j}{m}+1\right], \quad \frac{1}{m}-\frac{1}{n} \leqslant \alpha_{j0} \leqslant \frac{1}{m}+\frac{1}{n}.$$

Hence the main term of (11) satisfies

$$\frac{\phi(n)}{2}c_{r,\delta}\alpha_{j0}\alpha_{k0} = \frac{\phi(n)}{2m^2}c_{r,\delta} + R_1, \quad |R_1| \leqslant \frac{3}{m}. \tag{14}$$

On the other hand, the geometric series in (13) can be easily summed. With $z = e(vm/n)$ we have

$$\alpha_{jv} = \frac{1}{n}e\left(-\frac{vj}{n}\right)\frac{1-z^{L+1}}{1-z},$$

thus

$$|\alpha_{jv}| = \frac{1}{n}\frac{|1-z^{L+1}|}{|1-z|} \leqslant \frac{1}{n}\frac{2}{|1-z|} = \frac{1}{n|\sin \pi vm/n|}$$

(we used the fact that $|1-e(t)| = 2|\sin \pi t|$). As v runs from 1 to $n-1$, the residue of vm modulo n assumes the values 1 to $n-1$, since $(m, n) = 1$, and we have $(vm, n) = (v, n)$. Hence

$$\begin{aligned}\sum_{v=1}^{n-1} |\alpha_{jv}|\sqrt{(v, n)} &\leqslant \frac{1}{n}\sum_{v=1}^{n-1} \frac{\sqrt{(v, n)}}{|\sin \pi vm/n|}\\ &= \frac{1}{n}\sum_{v=1}^{n-1} \frac{\sqrt{(v, n)}}{\sin \pi v/n}\\ &\leqslant \frac{2}{n}\sum_{v=1}^{[n/2]} \frac{\sqrt{(v, n)}}{\sin \pi v/n}.\end{aligned}$$

Since $\sin t \geqslant (2/\pi)t$ on $[0, \pi/2]$, this sum is

$$\leqslant \sum_{v=1}^{[n/2]} \frac{\sqrt{(v, n)}}{v} \ll 2^{\nu} \log n$$

by Lemma 3. Thus the first sum in estimate (12) of R is $O(2^{\nu} \log n)$, and by symmetry so is the second.

By the same arguments, the third sum can be estimated as follows:

$$\begin{aligned}\sum_{v=1}^{n-1}\sum_{w=1}^{n-1} |\alpha_{jv}\alpha_{kw}|\sqrt{(v, w, n)} &\leqslant \frac{1}{n^2}\sum_{v=1}^{n-1}\sum_{w=1}^{n-1} \frac{\sqrt{(v, w, n)}}{|\sin \pi vm/n \sin \pi wm/n|}\\ &= \frac{1}{n^2}\sum_{v=1}^{n-1}\sum_{w=1}^{n-1} \frac{\sqrt{(v, w, n)}}{\sin \pi v/n \sin \pi w/n}\\ &\leqslant \frac{4}{n^2}\sum_{v=1}^{[n/2]}\sum_{w=1}^{[n/2]} \frac{\sqrt{(v, w, n)}}{\sin \pi v/n \sin \pi w/n}\\ &\leqslant \sum_{v=1}^{[n/2]}\sum_{w=1}^{[n/2]} \frac{\sqrt{(v, w, n)}}{vw}\\ &\ll (\log n)^2\end{aligned}$$

by Lemma 4.

Substituting these estimates into (12) we obtain

$$|R| \ll 2^{\nu}\sqrt{n}(\log n)^2. \tag{15}$$

Theorem 2 follows from (12), (14) and (15). ∎

References

1. Chaładus, S.: An application of Nagell's estimate for the least quadratic non-residue, *Demonstratio Math.*, to appear.
2. Hasse, H.: *Vorlesungen über Zahlentheorie*, Berlin, 1950.
3. Malyshev, A. V.: A generalization of Kloosterman sums and their estimates (in Russian), *Vestnik Leningrad. Univ.* 15 (1960) No. 13, vypusk 3, 59–75.
4. Terjanian, G.: Letter to A. Schinzel of February 15, 1993.
5. Wenpeng, Zhang: On a problem of D. M. Lehmer and its generalization, *Compositio Math.* 86 (1993) 307–316.