Bollettino
Unione Matematica Italiana

P. Codecá, M. Nair

Links between $\Delta(x,N)=\sum_{n\le xN,\ (n,N)=1} 1 - x\phi(N)$ and character sums

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **6-B** (2003), n.2, p. 509–516.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2003_8_6B_2_509_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2003.

Bollettino U. M. I.
(8) **6**-B (2003), 509-516

Links between $\Delta(x,N) = \sum_{\substack{n \leqslant xN \\ (n,N)=1}} 1 - x\varphi(N)$ and Character Sums (*).

P. CODECÁ - M. NAIR

Sunto. – *Esprimiamo la funzione* $\Delta(x, N)$ *definita nel titolo, per* $x = \frac{a}{q}$ *con* q *primo, mediante i caratteri modulo* q. *Utilizzando questo risultato dimostriamo che il confine inferiore universale per* $\Delta(N) = \sup_{x \in \boldsymbol{R}} |\Delta(x, N)|$ *può, in generale, essere sostanzialmente migliorato quando* N *è composto di primi che appartengono ad una fissata classe di resti modulo* q. *Otteniamo inoltre un analogo miglioramento nel caso in cui* N *sia il prodotto dei primi* s *primi, per infiniti valori di* s.

Summary. – *We express* $\Delta(x, N)$, *as defined in the title, for* $x = \frac{a}{q}$ *and* q *prime in terms of values of characters modulo* q. *Using this, we show that the universal lower bound for* $\Delta(N) = \sup_{x \in \boldsymbol{R}} |\Delta(x, N)|$ *can, in general, be substantially improved when* N *is composed of primes lying in a fixed residue class modulo* q. *We also prove a corresponding improvement when* N *is the product of the first* s *primes for infinitely many natural numbers* s.

Introduction.

The function $\Delta(x, N)$ is defined for $x \in \boldsymbol{R}$ and $N > 1$ by

$$\Delta(x, N) = \sum_{\substack{n \leqslant xN \\ (n, N) = 1}} 1 - x\varphi(N)$$

where $\varphi(N)$ is Euler's function. In an earlier paper [1], we proved a number of results on this interesting function and, in particular, on its extremal value $\Delta(N)$ defined by

$$\Delta(N) = \sup_{x} |\Delta(x, N)|.$$

(*) AMS subject classification: 11 N 25.

These include

(i) $\Delta(x, N)$ is periodic in x of period 1,

(ii) for squarefree N,

$$\Delta(x, N) = -\mu(N) \sum_{d|N} \mu(d)\, P(xd)$$

where μ is the Möbius function and $P(t)$ denotes the first Bernouilli polynomial defined by

$$P(t) = \begin{cases} t - [t] - 1/2\,, & t \notin \boldsymbol{Z}\,, \\ 0\,, & \text{otherwise}\,, \end{cases}$$

(iii) $\Delta(N) \leqslant 2^{\omega(N)-1}$,

(iv) $\Delta(N) \geqslant \left(\frac{1}{12} 2^{\omega(N)} \frac{\varphi(N)}{N}\right)^{1/2}$,

and

(v) if $p \nmid N$, p prime, then

(a) $\Delta(Np) \geqslant \left(1 - \frac{1}{p}\right) \Delta(N)$ and

(b) $\Delta(Np) \leqslant 2\Delta(N) - \frac{1}{p}$.

Here $\omega(N)$ denotes the number of distinct prime factors of N. The assertion (iii) is indeed best possible while it is extremely unlikely that this is the case for (iv).

In this paper which may be viewed as a continuation of [1], we derive a new expression for $\Delta(x, N)$ for rational $x = a/q$ in terms of characters modulo q. Using this we show that in the particular case when N is divisible exclusively by primes lying in a fixed residue class, the universal lower bound (iv) above can be, in general, substantially improved. An interesting ingredient in this approach is the use of the classical Dirichlet class number formula. We also show using an oscillation theorem due to Ingham together with property (v)(a) above that for the special case when N is the product of the first s primes, we can again improve (iv) for infinitely many such N. This result is significant since it can easily be shown that Ω results for such N have an implication for all N whose prime factors are among the first s primes.

Preliminaries and results.

Let q be a fixed odd prime and $P(t)$ be as described in the introduction. Since the characters modulo q, denoted by $\chi_m(n)$, $1 \leqslant m \leqslant q-1$, satisfy the orthogonality relationship

$$\sum_{n=1}^{q-1} \chi_i(n)\, \overline{\chi_j(n)} = \begin{cases} q-1\,, & \text{if } i = j \\ 0\,, & \text{otherwise}\,, \end{cases}$$

and are periodic modulo q, the odd periodic function $P\left(\frac{n}{q}\right)$ of period q can be expressed as

$$P\left(\frac{n}{q}\right) = \sum_{m=1}^{q-1} g(m)\, \chi_m(n) \tag{1}$$

where the coefficients $g(m)$ are zero when m is even (since only odd characters are required in the expansion) and are given by

$$g(m) = \frac{1}{q-1} \sum_{n=1}^{q-1} P\left(\frac{n}{q}\right) \overline{\chi_m(n)} \tag{2}$$

for m odd. We also recall that for any n with $q \nmid n$, we can write $\chi_m(n)$ as

$$\chi_m(n) = e^{2\pi i m \frac{\nu(n)}{q-1}} \tag{3}$$

where $\nu(n)$ is the exponent of n with respect to a fixed primitive root modulo q.

Observe that the classical class number formula ([3], pag. 37)

$$L(1, \chi) = \frac{i\pi}{q} S(\chi) \sum_{n=1}^{q-1} \overline{\chi(n)} P\left(\frac{n}{q}\right)$$

for each odd character χ modulo q implies via $L(1, \chi) \neq 0$ that the sum in (2) and hence the coefficients $g(m)$ also in (2) are nonzero for odd m.

Another simple observation which arises directly from the orthogonality of characters is that for any subset S of $\{1, \ldots, q-1\}$ and $c(m) \in \boldsymbol{C}$, we have that

$$\sum_{m \in S} c(m)\, \chi_m(a) = 0 \ \forall a,\ 1 \leqslant a \leqslant q-1 \Rightarrow c(m) = 0 \ \forall m \in S\,. \tag{4}$$

Using (ii) above, applied to $x = a/q$ and for squarefree N, yields

$$\Delta\left(\frac{a}{q}, N\right) = -\mu(N) \sum_{d \mid N} \mu(d)\, P\left(\frac{ad}{q}\right).$$

Substituting $P\left(\frac{ad}{q}\right)$ in the form given by (1) and simplifying with the complete multiplicativity of characters now readily leads to our new expression for

$\Delta\left(\frac{a}{q}, N\right)$ announced earlier

$$\Delta\left(\frac{a}{q}, N\right) = -\mu(N) \sum_{n=1}^{q-1} g(m)\,\chi_m(a) \prod_{p|N} (1-\chi_m(p)). \tag{5}$$

Although we have chosen to state this expression only for q an odd prime as required for our application, one can indeed derive a more convoluted version of (5) valid for more general q.

THEOREM 1. – Let q be an odd prime, $r \in \boldsymbol{N}$ with $1 \leqslant r \leqslant q-1$ and N a squarefree integer whose prime factors are all congruents to r modulo q. Let κ denote the order of r modulo q. Then we have

$$\Delta(N) \geqslant \begin{cases} c_q 2^{\omega(N)}, & \text{if } \kappa \equiv 2 (\mathrm{mod}\, 4) \\ c_q \left(2\cos\dfrac{\pi}{\kappa}\right)^{\omega(N)}, & \text{if } \kappa \equiv 0 (\mathrm{mod}\, 4) \\ c_q \left(2\cos\dfrac{\pi}{2\kappa}\right)^{\omega(N)}, & \text{if } \kappa \equiv 1 (\mathrm{mod}\, 2). \end{cases}$$

Here c_q denotes a positive constant depending at most on q which is not necessarily the same at each occurrence.

PROOF. – From the definition of $\Delta(N)$, we deduce via (5) that

$$\Delta(N) \geqslant \left| \sum_{m=1}^{q-1} g(m)\,\chi_m(a) \prod_{p|N} (1-\chi_m(p)) \right| \tag{6}$$

for any a, $1 \leqslant a \leqslant q-1$.

As noted before in (3), if h is a fixed primitive root modulo q, $\chi_m(p) = e^{2\pi i m \frac{\nu(p)}{q-1}}$ where $h^{\nu(p)} \equiv p \equiv r (\mathrm{mod}\, q)$ and hence $\kappa\nu(p) = \lambda(p)(q-1)$ for some $\lambda(p) \in \boldsymbol{N}$. Further $(\lambda(p), \kappa) = 1$ since otherwise $r^{\kappa/(\lambda(p), \kappa)} \equiv 1 (\mathrm{mod}\, q)$ which contradicts the definition of κ. An easy simplification yields

$$1 - \chi_m(p) = -2ie^{\pi i m \frac{\nu(p)}{q-1}} \sin\frac{\pi m \nu(p)}{q-1}.$$

The argument now breaks up into the stated three cases.

CASE 1: $\kappa \equiv 2 (\mathrm{mod}\, 4)$.

Since $(\lambda(p), \kappa) = 1$, $\lambda(p)$ is odd in this case and writing $q - 1 = 2^{\alpha} m_1$, where $\alpha \in \boldsymbol{N}$ and m_1 is odd, we deduce from $\kappa\nu(p) = \lambda(p)(q-1)$ that $\nu(p) = 2^{\alpha-1} M$ where M is odd. We observe that the term in (6) corresponding to the odd value $m = m_1$ has

$$|1 - \chi_{m_1}(p)| = 2 \left| \sin \frac{\pi m_1 \nu(p)}{q-1} \right| = 2 \left| \sin \frac{M\pi}{2} \right| = 2$$

and hence is

$$2^{\omega(N)} g(m_1)\, \chi_{m_1}(a)\, e^{i\vartheta_1}$$

for some real ϑ_1. All other possible odd values of m, say $m_2, \ldots, m_k$, which also yield such terms involving $2^{\omega(N)}$ give rise to a total contribution of

$$2^{\omega(N)} \sum_{j=1}^{k} g(m_j)\, \chi_{m_j}(a)\, e^{i\vartheta_j}, \qquad \vartheta_j \in \boldsymbol{R},$$

which by observation (4) yields, in absolute value, $c_q 2^{\omega(N)}$ for some strictly positive constant c_q. Using now the lower bound given by the triangle inequality to dispose off the contributions from all other values of m, we deduce in conclusion that

$$\Delta(N) \geqslant c_q 2^{\omega(N)}.$$

This completes Case 1. This kind of reasoning also applies to the other two cases and so we shall restrict ourself to pointing out the dominant values of m and their contributions to (6).

CASE 2: $\kappa \equiv 0 (\mathrm{mod}\, 4)$.

Again, $\lambda(p)$ is odd in this case. Since $(\lambda(p), \kappa) = 1$, we can solve the congruence $m\lambda(p) \equiv 2k + 1 (\mathrm{mod}\, \kappa)$, where $\kappa = 4k$ with $k \in \boldsymbol{N}$. Clearly since the right hand side is odd, so is the solution $m = m_1$. For this m_1, we have that

$$\frac{m_1 \nu(p)}{q-1} = \frac{m_1 \lambda(p)}{\kappa} \equiv \frac{2k+1}{4k} (\mathrm{mod}\, 1).$$

Since $\dfrac{2k+1}{4k} = \dfrac{1}{2} + \dfrac{1}{4k}$, we obtain that

$$\left| \sin \frac{\pi m_1 \nu(p)}{q-1} \right| = \left| \sin \left(\frac{\pi}{2} + \frac{\pi}{4k} \right) \right| = \left| \cos \frac{\pi}{4k} \right| = \left| \cos \frac{\pi}{\kappa} \right|$$

and hence $|1 - \chi_{m_1}(p)| = \left| 2 \cos \dfrac{\pi}{\kappa} \right|$.

The rest of the argument proceeds as in Case 1.

CASE 3: $\kappa \equiv 1 (\mathrm{mod}\, 2)$.

Writing $\kappa = 2k + 1$, $k \in \boldsymbol{N}$, again as in Case 2 we can solve $m\lambda(p) \equiv k (\mathrm{mod}\, \kappa)$ but the solution $m = m_1$ can unfortunately be even. However, in this case, $\kappa - m_1$ is a solution of $m\lambda(p) \equiv k+1 (\bmod \kappa)$ and either m_1 or $\kappa - m_1$ is odd. Hence for some choice of $\pm$, we can solve $m\lambda(p) \equiv \pm k (\bmod \kappa)$ with odd m.

For this solution, we have that

$$\frac{m\nu(p)}{q-1} = \frac{m\lambda(p)}{\kappa} \equiv \frac{\pm k}{2k+1} (\bmod 1).$$

Hence

$$\left| \sin \frac{\pi m \nu(p)}{q-1} \right| = \left| \sin \left(\pm \frac{\pi}{2} \mp \frac{\pi}{2(2k+1)} \right) \right| = \left| \cos \frac{\pi}{2\kappa} \right|$$

so that

$$|1 - \chi_m(p)| = 2 \left| \cos \frac{\pi}{2\kappa} \right|.$$

The argument now continues as in the other cases.

This completes the proof of Theorem 1.

REMARK 1. – A closer examination of the proof in Case 1 reveals that since the dominant choice of m depends only on $q-1$ and not on r, the result in this case remains true even if all the prime factors of N lie in different residue classes modulo q provided that all the orders concerned are congruent to 2 modulo 4.

REMARK 2. – Given any odd squarefree N, we can actually find an odd prime q with the property that all the orders modulo q of the prime factors of N are congruent to 2 modulo 4. To see this, denote, for each $p|N$, R_p and N_p to be typical quadratic residues and non-residues modulo p respectively. For each $p \equiv 3 (\bmod 4)$, we require that q satisfies $q \equiv 3 (\bmod 4)$ and $q \equiv R_p (\bmod p)$ and for each $p \equiv 1 (\bmod 4)$, we require that $q \equiv 3 (\bmod 4)$ and $q \equiv N_p (\bmod p)$. The Chinese Remainder Theorem and Dirichlet's theorem on primes in arithmetic progressions ensure that such primes q exist. An easy computation using the Quadratic Reciprocity Theorem then shows that q does indeed have the property stated. Unfortunately, realistic estimates for the size of such a q appear to be very difficult to obtain and this effectively prevents a concrete application of this approach.

REMARK 3. – From (5), we deduce that for squarefree N,

$$\left| \Delta \left(\frac{a}{q}, N \right) \right|^2 = \sum_{m_1, m_2 = 1}^{q-1} g(m_1)\, \overline{g(m_2)}\, \chi_{m_1}(a)\, \overline{\chi_{m_2}(a)} \prod_{p|N} (1 - \chi_{m_1}(p))(1 - \overline{\chi_{m_2}(p)}).$$

On summing over a, $1 \leqslant a \leqslant q-1$, and simplifying, we obtain

$$\sum_{a=1}^{q-1} \left| \Delta\left(\frac{a}{q}, N\right) \right|^2 = (q-1) \sum_{m=1}^{q-1} |g(m)|^2 \prod_{p|N} |1-\chi_m(p)|^2$$

which, using (2) and the class number formula, leads to the curious identity

$$\sum_{a=1}^{q-1} \left| \Delta\left(\frac{a}{q}, N\right) \right|^2 = \frac{1}{\pi^2} \frac{q}{q-1} \sum_{\substack{m=1 \\ m \text{ odd}}}^{q-1} |L(1, \chi_m)|^2 \prod_{p|N} |1-\chi_m(p)|^2.$$

THEOREM 2. – Let $s \in \boldsymbol{N}$ and denote by N_s the product of the first s primes. Then for infinitely many s,

$$\Delta(N_s) \geqslant c \cdot 2^{\frac{s}{2}} 2^{c_1 s^{1/2} \frac{\log\log\log s}{(\log s)^{1/2}}}$$

where c and c_1 are positive constants.

PROOF. – We shall need two results from our previous paper [1] namely Theorem 2 and Theorem 4 (iii). These imply that any integer N with all prime factors congruents to 3 modulo 4 satisfies $\Delta(N) \geqslant \frac{1}{4} 2^{\omega(N)}$ and that for any N and a prime p with $p \nmid N$ we have that

$$\Delta(Np) \geqslant \left(1 - \frac{1}{p}\right) \Delta(N).$$

Writing $N_s = 2M_1M_3$ where M_1 is divisible only by primes which are congruent to 1 modulo 4 and M_3 only by primes which are congruent to 3 modulo 4 and using $\Delta(2N) = \Delta(N)$ for any odd N, we therefore deduce

$$\Delta(N_s) \geqslant \prod_{p|M_1} \left(1 - \frac{1}{p}\right) \Delta(M_3) \geqslant \frac{1}{4} \prod_{p|M_1} \left(1 - \frac{1}{p}\right) 2^{\omega(M_3)}.$$

Writing x for the s^{th} prime, standard estimates yield

$$\Delta(N_s) \geqslant c \frac{1}{(\log x)^{1/2}} 2^{\pi_3(x)} \tag{7}$$

where $\pi_3(x)$ denotes the number of primes $\leqslant x$ which are congruent to 3 modulo 4. An oscillation theorem due to Ingham [2], p. 107 implies that

$$\pi_3(x) \geqslant \frac{s}{2} + c_1 \frac{x^{1/2} \log\log\log x}{\log x}.$$

The result now follows on substituting this in (7) and using $x \sim s \log s$.

REFERENCES

[1] P. Codecà - M. Nair, *Extremal Values of* $\Delta(x, N) = \sum_{\substack{n \leqslant xN \\ (n, N) = 1}} 1 - x\varphi(N)$. *Canad. Math. Bull. Vol.*, **41** (3), (1998), 335-347.

[2] A. E. Ingham, *The Distribution of Prime Numbers*, Hafner Publishing Company, New York 1971.

[3] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, Springer-Verlag, New York 1982.

P. Codecà: Dipartimento di Matematica, Università di Ferrara
Via Machiavelli 35, 44100 Ferrara, Italy; e-mail: cod@dns.unife.it

M. Nair: Department of Mathematics, University of Glasgow
Glasgow G12 8QW, U.K.; e-mail: m.nair@maths.gla.ac.uk

Pervenuta in Redazione
il 31 agosto 2001