SELBERG'S IDENTITY FOR KLOOSTERMAN SUMS

GERGELY HARCOS AND GYULA KÁROLYI

1. Introduction

In this note, we give a simple and self-contained proof of Selberg's identity for the Kloosterman sum

$$S(m,n;q) := \sum_{x \pmod q}^{*} e\left(\frac{mx+n\overline{x}}{q}\right). \tag{1}$$

Here, x runs through the reduced residues modulo q, $\overline{x}$ is the multiplicative inverse of x modulo q, and $e(t) := \exp(2\pi it)$ denotes the standard additive character of the circle group $\mathbb{R}/\mathbb{Z}$. The identity was stated without proof by Selberg in his early paper [4], rediscovered by Kuznetsov [2, Theorem 4] through his famous formula, and proved in an elementary way by Matthes [3] and Andersson [1, Part III]:

Theorem. *For any positive integer q, and for any integers m and n, we have*

$$S(m,n;q) = \sum_{d\mid(m,n,q)} d\, S\left(1,\frac{mn}{d^2};\frac{q}{d}\right). \tag{2}$$

2. The proof

For the proof of the above Theorem, let us denote by $P(q)$ the statement that (2) holds for all $m,n\in\mathbb{Z}$. Then, clearly, it suffices to show the following two results.

Lemma 1. *If q_1 and q_2 are coprime positive integers, then $P(q_1)$ and $P(q_2)$ imply $P(q_1q_2)$.*

Lemma 2. *$P(p^\alpha)$ is true for any prime p and any nonnegative integer α.*

Proof of Lemma 1. Let us denote $q := q_1q_2$, and let $m,n\in\mathbb{Z}$ be arbitrary. We start from the well-known identity[1]

$$S(m,n;q) = S(m,n\overline{q_2}^2;q_1)S(m,n\overline{q_1}^2;q_2), \tag{3}$$

where $\overline{q_2}$ is the multiplicative inverse of q_2 modulo q_1, and $\overline{q_1}$ is the multiplicative inverse of q_1 modulo q_2. To prove this identity, we represent x in (1) as $x = x_1q_2 + x_2q_1$, where $x_1 \pmod{q_1}$ and $x_2 \pmod{q_2}$ are uniquely determined reduced residues. Then, it is straightforward to verify that

$$\overline{x} \equiv \overline{q_2}^2\,\overline{x_1}\,q_2 + \overline{q_1}^2\,\overline{x_2}\,q_1 \pmod q,$$

whence

$$e\left(\frac{mx+n\overline{x}}{q}\right) = e\left(\frac{mx_1+n\overline{q_2}^2\overline{x_1}}{q_1}\right)e\left(\frac{mx_2+n\overline{q_1}^2\overline{x_2}}{q_2}\right),$$

[1] usually written in the more symmetric form $S(m,n;q) = S(m\overline{q_2},n\overline{q_2};q_1)S(m\overline{q_1},n\overline{q_1};q_2)$

and (3) follows. Combining (3) with $P(q_1)$ and $P(q_2)$, we obtain

$$\begin{aligned} S(m,n;q) &= \sum_{\substack{d_1\mid(m,n\overline{q_2}^2,q_1)\\ d_2\mid(m,n\overline{q_1}^2,q_2)}} d_1d_2\, S\left(1,\frac{mn\overline{q_2}^2}{d_1^2};\frac{q_1}{d_1}\right) S\left(1,\frac{mn\overline{q_1}^2}{d_2^2};\frac{q_2}{d_2}\right)\\ &= \sum_{\substack{d_1\mid(m,n,q_1)\\ d_2\mid(m,n,q_2)}} d_1d_2\, S\left(1,\frac{mn(\overline{q_2}d_2)^2}{(d_1d_2)^2};\frac{q_1}{d_1}\right) S\left(1,\frac{mn(\overline{q_1}d_1)^2}{(d_1d_2)^2};\frac{q_2}{d_2}\right). \end{aligned}$$

In the last sum, we observe that $\overline{q_2}d_2$ is the multiplicative inverse of q_2/d_2 modulo q_1/d_1, while $\overline{q_1}d_1$ is the multiplicative inverse of q_1/d_1 modulo q_2/d_2. Therefore, adapting (3) for the product of the last two Kloosterman sums, and introducing the notation $d := d_1d_2$, we arrive at

$$\begin{aligned} S(m,n;q) &= \sum_{\substack{d_1\mid(m,n,q_1)\\ d_2\mid(m,n,q_2)}} d_1d_2\, S\left(1,\frac{mn}{(d_1d_2)^2};\frac{q_1q_2}{d_1d_2}\right)\\ &= \sum_{d\mid(m,n,q)} d\, S\left(1,\frac{mn}{d^2};\frac{q}{d}\right). \end{aligned}$$

That is, $P(q)$ holds, and we are done. The proof Lemma 1 is complete. □

Proof of Lemma 2. We fix the prime p, and proceed by induction on α. We want to prove $P(p^\alpha)$. For $\alpha=0$ the statement is trivial, so we assume that $\alpha\geqslant 1$ and $P(p^{\alpha-1})$ holds. Let us denote $q := p^\alpha$, and let $m,n\in\mathbb{Z}$ be arbitrary. If $(m,p)=1$ or $(n,p)=1$, we get from (1) by a simple change of variable that $S(m,n;q)=S(1,mn;q)$, which is (2) in this situation. So from now on we assume that p divides both m and n. Then, using also the induction hypothesis $P(p^{\alpha-1})$, the equation (2) that we want to prove simplifies to

$$S(m,n;q) = S(1,mn;q) + pS\left(\frac{m}{p},\frac{n}{p};\frac{q}{p}\right). \tag{4}$$

For $\alpha=1$, i.e. $q=p$, equation (4) is valid, because it is straightforward that

$$S(m,n;p)=p-1, \qquad S(1,mn;p)=-1, \qquad S\left(\frac{m}{p},\frac{n}{p};1\right)=1.$$

So from now on we assume that $\alpha\geqslant 2$. Then, in the definition (1), the coprimality condition $(x,q)=1$ is equivalent to $(x,q/p)=1$, whence in (4) the left hand side is equal to the second term on the right hand side. That is, (4) simplifies further to $S(1,mn;q)=0$. Note that here $p^2\mid mn$ by assumption. More generally, we shall show the following:

$$S(1,r;p^\alpha)=0 \qquad \text{whenever} \qquad p\mid r \text{ and } \alpha\geqslant 2. \tag{5}$$

We verify (5) by direct calculation. According to the definition (1),

$$S(1,r;q) = \sideset{}{^*}\sum_{x \pmod q} e\left(\frac{x+r\overline{x}}{q}\right).$$

Here, $q=p^\alpha$ is a prime power divisible by p^2, and r is divisible by p. We claim that the map $x\mapsto x+r\overline{x}$ permutes the reduced residues modulo q. Clearly, $x+r\overline{x}$ is always coprime to q, hence it suffices to check that the map is injective modulo q. Assuming

$$x+r\overline{x}\equiv y+r\overline{y} \pmod q,$$

where x and y are coprime to q, we infer

$$\begin{aligned} (x-y)+r(\overline{x}-\overline{y}) &\equiv 0 \pmod q,\\ xy(x-y)+r(y-x) &\equiv 0 \pmod q,\\ (xy-r)(x-y) &\equiv 0 \pmod q. \end{aligned}$$

In the last congruence, $xy-r$ is coprime to q, whence $x \equiv y \pmod q$ as claimed. From here (5) is immediate:

$$S(1,r;q) = \sum_{k \pmod q}^{*} e\left(\frac{k}{q}\right) = \sum_{1 \leqslant k \leqslant q} e\left(\frac{k}{q}\right) - \sum_{\substack{1 \leqslant k \leqslant q \\ p \mid k}} e\left(\frac{k}{q}\right) = 0 - 0 = 0.$$

The proof Lemma 2 is complete. □

3. Concluding remarks

The proof of Lemma 2 shows that, for a prime power modulus $q = p^{\alpha}$, all but the last two terms in Selberg's identity (2) vanish. More precisely, if either m or n is not divisible by q, then $d := (m,n,q)$ is the only divisor that contributes to (2). If m and n are both divisible by q, then the divisors $d = q$ and $d = q/p$ contribute (q and $-q/p$, respectively), but the others do not. By refining this observation and combining it with the proof of Lemma 1, we can see that, for a general modulus q, only those divisors $d \mid (m,n,q)$ contribute to (2) for which both $(m,q)/d$ and $(n,q)/d$ are square-free. For example, in the special case $n = 0$, Selberg's identity (2) yields the usual evaluation of Ramanujan sums:

$$S(m,0;q) = \sum_{d \mid (m,q)} d\, S\left(1,0;\frac{q}{d}\right) = \sum_{d \mid (m,q)} d\, \mu\left(\frac{q}{d}\right).$$

4. Acknowledgements

First author supported by NKFIH (National Research, Development and Innovation Office) grants NK 104183, ERC_HU_15 118946, K 119528, and by the MTA Rényi Intézet Lendület Automorphic Research Group. Second author supported by NKFIH (National Research, Development and Innovation Office) grants K 119528 and K 120154.

References

[1] J. Andersson, *Summation formulae and zeta functions*, Ph.D. thesis, Stockholm University, 2006, available at http://www.diva-portal.org

[2] N. V. Kuznecov, *The Petersson conjecture for cusp forms of weight zero and the Linnik conjecture. Sums of Kloosterman sums*, Math. USSR Sbornik **39** (1981), 299–342.

[3] R. Matthes, *An elementary proof of a formula of Kuznecov for Kloosterman sums*, Results Math. **18** (1990), 120–124.

[4] A. Selberg, *Über die Fourierkoeffizienten elliptischer Modulformen negativer Dimension*, C. R. Neuvième Congrès Math. Scandinaves, Helsingfors (1938), 320–322, In: Collected papers I, Springer-Verlag, Berlin, 1989.

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, POB 127, Budapest H-1364, Hungary
E-mail address: `harcos.gergely@renyi.mta.hu`

MTA Rényi Intézet Lendület Automorphic Research Group
E-mail address: `harcos.gergely@renyi.mta.hu`

Central European University, Nador u. 9, Budapest H-1051, Hungary
E-mail address: `harcosg@ceu.hu`

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, POB 127, Budapest H-1364, Hungary
E-mail address: `karolyi.gyula@renyi.mta.hu`

Institute of Mathematics, Eötvös University, Pázmány P. sétány 1/C, Budapest H-1117, Hungary
E-mail address: `karolyi@cs.elte.hu`