BULL. AUSTRAL. MATH. SOC. 11L05, 11L40, 11T24
VOL. 75 (2007) [221–227]

ON THE DISTRIBUTION OF ANGLES OF THE SALIÉ SUMS

IGOR E. SHPARLINSKI

For a prime p and integers a and b, we consider Salié sums

$$S_p(a,b) = \sum_{x=1}^{p-1} \chi_2(x) \exp\bigl(2\pi i(ax + b\overline{x})/p\bigr),$$

where $\chi_2(x)$ is a quadratic character and $\overline{x}$ is the modular inversion of x, that is, $x\overline{x} \equiv 1 \pmod p$. One can naturally associate with $S_p(a,b)$ a certain angle $\vartheta_p(a,b) \in [0,\pi]$. We show that, for any fixed $\varepsilon > 0$, these angles are uniformly distributed in $[0,\pi]$ when a and b run over arbitrary sets $\mathcal{A}, \mathcal{B} \subseteq \{0,1,\dots,p-1\}$ such that there are at least $p^{1+\varepsilon}$ quadratic residues modulo p among the products ab, where $(a,b) \in \mathcal{A}\times\mathcal{B}$.

1. INTRODUCTION

For a prime $p \geqslant 3$ and integers a and b, we consider Salié sums

$$S_p(a,b) = \sum_{x=1}^{p-1} \chi_2(x) \mathbf{e}_p(ax + b\overline{x}),$$

where $\chi_2(x)$ is a quadratic character, $\overline{x}$ is the modular inversion of x, that is, $x\overline{x} \equiv 1 \pmod p$, and

$$\mathbf{e}_p(z) = \exp(2\pi i z/p).$$

One can naturally associate with $S_p(a,b)$ a certain angle $\vartheta_p(a,b)$. It is known, see [**7, 15**] that for integers a and b with $\gcd(ab,p) = 1$ we have

$$S_p(a,b) = G_p(a) \sum_{\substack{u=1 \\ u^2 \equiv 4ab \pmod p}}^{p-1} \mathbf{e}_p(u)$$

where

$$G_p(a) = \sum_{x=0}^{p-1} \mathbf{e}_p(ax^2)$$

Received 4th September, 2006

https://doi.org/10.1017/S0004972700039150 Published online by Cambridge University Press

is the Gauss sum. Thus $S_p(a,b)$ vanishes if $\chi_2(ab) = -1$ and

$$S_p(a,b) = G_p(a)\cos\Big(\frac{2\pi u_p(a,b)}{p}\Big) = G_p(b)\cos\Big(\frac{2\pi u_p(a,b)}{p}\Big)$$

if $\chi_2(ab) = 1$, where $u_p(a,b)$ is the smallest solution to the following congruence:

$$u^2 \equiv 4ab \pmod p, \qquad 1 \leqslant u \leqslant p-1. \tag{1}$$

Thus it is natural to say that

$$\vartheta_p(a,b) = \frac{2\pi u_p(a,b)}{p}$$

is the *angle* of the Salié sum $S_p(a,b)$.

Duke, Friedlander and Iwaniec [**4**] and Tóth [**17**] using very deep arguments, show that if a and b are fixed integers, then the sequence of the angles $\vartheta_p(a,b)$ is uniformly distributed in the interval $[0,\pi]$ when p runs through the primes such that ab is a quadratic residue modulo p.

Here we show that a similar result also holds for the case when a sufficiently large prime p is fixed and a and b run through arbitrary sets of integers $\mathcal{A}$ and $\mathcal{B}$ which both have some sufficiently many quadratic residues or non-residues. For example, $\mathcal{A}$ and $\mathcal{B}$, could consist of consecutive integers each (for arbitrary $\varepsilon > 0$).

It is useful to recall, that *Kloosterman sums*

$$K_p(a,b) = \sum_{x=1}^{p-1} \mathbf{e}_p(ax + b\overline{x}),$$

which are very close relatives of Salié sums, exhibit a very different behaviour described by the *Sato–Tate* conjecture. See [**1, 3, 5, 6, 8, 9, 10, 12, 13, 14, 16**] for various modifications and generalisations of this conjecture and further references.

Throughout the paper, the implied constants in the symbols 'O', and '$\ll$' are absolute. We recall that the notations $U = O(V)$ and $U \ll V$ are both equivalent to the assertion that the inequality $|U| \leqslant cV$ holds for some constant $c > 0$.

2. Distribution of Square Roots of Products

It is clear that the question of studying $\vartheta_p(a,b)$ with $a \in \mathcal{A}$ and $b \in \mathcal{B}$ is equivalent to the question of studying the distribution of solutions to the congruence (1).

Given two sets $\mathcal{A}, \mathcal{B} \subseteq \{0, 1, \dots, p-1\}$ we study the uniformity of distribution of the sequence of fractions u/p, where u runs through all solutions to the congruence (1), taken over all pairs $(a,b) \in \mathcal{A} \times \mathcal{B}$. That is, for a real $\gamma \in [0,1]$ we consider the counting function

$$N_{p,\gamma}(\mathcal{A},\mathcal{B}) = \sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}} \sum_{\substack{u=1 \\ u^2 \equiv 4ab \pmod p \\ u/p \leqslant \gamma}}^{p-1} 1$$

https://doi.org/10.1017/S0004972700039150 Published online by Cambridge University Press

and put for brevity

$$N_p(\mathcal{A},\mathcal{B}) = N_{p,1}(\mathcal{A},\mathcal{B}).$$

One sees that $N_p(\mathcal{A},\mathcal{B})$ is twice the number of pairs $(a,b) \in \mathcal{A}\times\mathcal{B}$ with $\chi_2(ab) = 1$.

We now define the *discrepancy* of the sequence of solutions to the congruence (1) for $(a,b)\in\mathcal{A}\times\mathcal{B}$:

$$D_p(\mathcal{A},\mathcal{B}) = \max_{0\leqslant\gamma<1}\left|\frac{N_{p,\gamma}(\mathcal{A},\mathcal{B})}{N_p(\mathcal{A},\mathcal{B})} - \gamma\right|.$$

THEOREM 1. *For any two sets* $\mathcal{A},\mathcal{B}\subseteq\{0,1,\dots,p-1\}$, *we have*

$$D_p(\mathcal{A},\mathcal{B}) \ll \sqrt{\frac{p}{N_p(\mathcal{A},\mathcal{B})}}\log p.$$

PROOF: We fix some $\gamma\in[0,1)$ and note that for $h = \lfloor\gamma p\rfloor$, we can write $N_{p,\gamma}(\mathcal{A},\mathcal{B})$ as

$$N_{p,\gamma}(\mathcal{A},\mathcal{B}) = \sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{\substack{u=1\\ u^2\equiv 4ab \pmod p}}^{h} 1 = \sum_{\nu=0}^{1}\sum_{a\in\mathcal{A}_\nu}\sum_{b\in\mathcal{B}_\nu}\sum_{\substack{u=1\\ u^2\equiv 4ab \pmod p}}^{h} 1, \tag{2}$$

where $\mathcal{A}_0,\mathcal{A}_1$ and $\mathcal{B}_0,\mathcal{B}_1$ are subsets of quadratic residues and non-residues among the elements of $\mathcal{A}$ and $\mathcal{B}$, respectively.

Let $\mathcal{X}$ be the set of all $p-1$ multiplicative characters modulo p. We recall the identity

$$\frac{1}{p-1}\sum_{\chi\in\mathcal{X}}\chi(c) = \begin{cases}1 & \text{if } c\equiv 1 \pmod p,\\ 0 & \text{otherwise,}\end{cases} \tag{3}$$

which holds for any integer c. Using (3), we write

$$\begin{aligned}\sum_{a\in\mathcal{A}_\nu}\sum_{b\in\mathcal{B}_\nu}\sum_{\substack{u=1\\ u^2\equiv 4ab \pmod p}}^{h} 1 &= \sum_{a\in\mathcal{A}_\nu}\sum_{b\in\mathcal{B}_\nu}\sum_{u=1}^{h}\frac{1}{p-1}\sum_{\chi\in\mathcal{X}}\chi(4ab\overline{u}^2)\\ &= \frac{1}{p-1}\sum_{\chi\in\mathcal{X}}\sum_{a\in\mathcal{A}_\nu}\sum_{b\in\mathcal{B}_\nu}\sum_{u=1}^{h}\chi(4ab\overline{u}^2),\end{aligned}$$

for $\nu = 0,1$. Clearly for for $\chi=\chi_0$ (the principal character) and also for $\chi=\chi_2$ we have $\chi(4ab\overline{u}^2) = 1$ over the whole area of summation over a, b and u. Hence,

$$\begin{aligned}&\sum_{a\in\mathcal{A}_\nu}\sum_{b\in\mathcal{B}_\nu}\sum_{\substack{u=1\\ u^2\equiv 4ab \pmod p}}^{h} 1\\ &\quad= 2\#\mathcal{A}_\nu\#\mathcal{B}_\nu\frac{h}{p-1} + \frac{1}{p-1}\sum_{\substack{\chi\in\mathcal{X}\\ \chi\neq\chi_0,\chi_2}}\chi(4)\sum_{a\in\mathcal{A}_\nu}\chi(a)\sum_{b\in\mathcal{B}_\nu}\chi(b)\sum_{u=1}^{h}\chi(\overline{u}^2).\end{aligned}$$

https://doi.org/10.1017/S0004972700039150 Published online by Cambridge University Press

If $\chi \neq \chi_0, \chi_2$ then $\psi(u) = \chi(\overline{u}^2)$ is a nonprincipal multiplicative character and by the *Polya–Vinogradov bound*, see [**7**, Theorems 12.5], we obtain

$$\sum_{u=1}^{h} \chi(\overline{u}^2) \ll p^{1/2} \log p.$$

Therefore,

(4)
$$\sum_{a\in\mathcal{A}_\nu} \sum_{b\in\mathcal{B}_\nu} \sum_{\substack{u=1 \\ u^2\equiv 4ab \pmod p}}^{h} 1 = 2\#\mathcal{A}_\nu \#\mathcal{B}_\nu \frac{h}{p-1} + O(W_\nu p^{-1/2} \log p),$$

where

(5)
$$W_\nu = \sum_{\chi\in\mathcal{X}} \left| \sum_{a\in\mathcal{A}_\nu} \chi(a) \right| \left| \sum_{b\in\mathcal{B}_\nu} \chi(b) \right|.$$

(Note that we have again extended the summation over all $\chi \in \mathcal{X}$.)

Furthermore, using the Cauchy inequality, we obtain

$$W_\nu^2 \leqslant \sum_{\chi\in\mathcal{X}} \left| \sum_{a\in\mathcal{A}_\nu} \chi(a) \right|^2 \sum_{\chi\in\mathcal{X}} \left| \sum_{b\in\mathcal{B}_\nu} \chi(b) \right|^2.$$

We recall that if $\gcd(c, q) = 1$, then for the conjugated character $\overline{\chi}$ we have $\overline{\chi}(c) = \chi(\overline{c})$. Therefore, by (3)

$$\sum_{\chi\in\mathcal{X}} \left| \sum_{a\in\mathcal{A}_\nu} \chi(a) \right|^2 = \sum_{\chi\in\mathcal{X}} \sum_{a_1,a_2\in\mathcal{A}_\nu} \chi(a_1 a_2) = \sum_{a_1,a_2\in\mathcal{A}_\nu} \sum_{\chi\in\mathcal{X}} \chi(a_1 \overline{a_2}) = (p-1)\#\mathcal{A}_\nu,$$

and similarly

$$\sum_{\chi\in\mathcal{X}} \left| \sum_{b\in\mathcal{B}_\nu} \chi(b) \right|^2 = (p-1)\#\mathcal{B}_\nu.$$

We now infer from (5) that

$$W_\nu \ll p\sqrt{\#\mathcal{A}_\nu \#\mathcal{B}_\nu}$$

which after substitution into (4) leads to the bound

(6)
$$\sum_{a\in\mathcal{A}_\nu} \sum_{b\in\mathcal{B}_\nu} \sum_{\substack{u=1 \\ u^2\equiv 4ab \pmod p}}^{h} 1 = 2\#\mathcal{A}_\nu \#\mathcal{B}_\nu \frac{h}{p-1} + O\left(\sqrt{\#\mathcal{A}_\nu \#\mathcal{B}_\nu p} \log p\right),$$

for $\nu = 0, 1$. Furthermore, as we have mentioned,

$$N_p(\mathcal{A}, \mathcal{B}) = 2(\#\mathcal{A}_0 \#\mathcal{B}_0 + \#\mathcal{A}_1 \#\mathcal{B}_1).$$

Hence, after substituting (6) in (2) we obtain

$$N_{p,\gamma}(\mathcal{A},\mathcal{B}) = N_p(\mathcal{A},\mathcal{B})\frac{h}{p-1} + O\Big(\sqrt{N_p(\mathcal{A},\mathcal{B})p}\log p\Big).$$

Since

$$\begin{aligned}N_p(\mathcal{A},\mathcal{B})\frac{h}{p-1} - \gamma N_p(\mathcal{A},\mathcal{B}) &\ll N_p(\mathcal{A},\mathcal{B})\Big(\frac{\gamma p + O(1)}{p-1} - \gamma\Big)\\ &\ll N_p(\mathcal{A},\mathcal{B})p^{-1} \ll \sqrt{N_p(\mathcal{A},\mathcal{B})p},\end{aligned}$$

the desired result follows. □

3. Angles of Salié Sums

Let for $0 \leqslant \alpha \leqslant \pi$ and two sets $\mathcal{A},\mathcal{B} \subseteq \{0,1,\ldots,p-1\}$, we denote by $T_{p,\alpha}(\mathcal{A},\mathcal{B})$ the number of $(a,b) \in \mathcal{A}\times\mathcal{B}$ with $\chi_2(ab) = 1$ for which

$$\vartheta_p(a,b) \leqslant \alpha,$$

and put for brevity

$$T_p(\mathcal{A},\mathcal{B}) = T_{p,\pi}(\mathcal{A},\mathcal{B}).$$

We now define the *discrepancy* of the sequence of solutions to the congruence (1) for $(a,b) \in \mathcal{A}\times\mathcal{B}$:

$$\Delta_p(\mathcal{A},\mathcal{B}) = \max_{0\leqslant\alpha<\pi}\left|\frac{T_{p,\alpha}(\mathcal{A},\mathcal{B})}{T_p(\mathcal{A},\mathcal{B})} - \alpha\right|.$$

Theorem 2. *For any two sets $\mathcal{A},\mathcal{B} \subseteq \{0,1,\ldots,p-1\}$, we have*

$$\Delta_p(\mathcal{A},\mathcal{B}) \ll \sqrt{\frac{p}{T_p(\mathcal{A},\mathcal{B})}}\log p.$$

Proof: Clearly

$$T_{p,\alpha}(\mathcal{A},\mathcal{B}) = N_{p,\alpha/2\pi}(\mathcal{A},\mathcal{B})$$

for $0 \leqslant \alpha < \pi$ and also

$$T_{p,\pi}(\mathcal{A},\mathcal{B}) = N_{p,1/2}(\mathcal{A},\mathcal{B}) = \frac{1}{2}N_p(\mathcal{A},\mathcal{B}).$$

Using Theorem 1 we immediately obtain the desired result. □

4. Comments

Clearly the asymptotic formulas of Theorems 1 and 2 are nontrivial under the condition

$$N_p(\mathcal{A}, \mathcal{B}) \geqslant p^{1+\varepsilon} \tag{7}$$

for any $\varepsilon > 0$ and sufficiently large p.

For example, if for some fixed $\varepsilon > 0$, the sets $\mathcal{A}$ and $\mathcal{B}$ consist of at least $p^{1/4+\varepsilon}$ consecutive integers each, then by the *Burgess bound*, see [**7**, Theorems 12.6],

$$N_p(\mathcal{A}, \mathcal{B}) = \left(\frac{1}{2} + o(1)\right)\#\mathcal{A}\#\mathcal{B}.$$

Furthermore, it follows from [**2**] that if for some fixed $\varepsilon > 0$, the sets $\mathcal{A}$ and $\mathcal{B}$ consist of at least $p^{1/4e^{1/2}+\varepsilon}$ consecutive integers each, then, for sufficiently large p,

$$N_p(\mathcal{A}, \mathcal{B}) \geqslant c(\varepsilon)\#\mathcal{A}\#\mathcal{B},$$

where $c(\varepsilon) > 0$ depends only on ε. Thus, if in addition we also have $\#\mathcal{A}\#\mathcal{B} \geqslant p^{1+\varepsilon}$ then the condition (7) is satisfied.

On the other hand, an example of the sets

$$\mathcal{A} = \mathcal{B} = \{a^2 \mid 1 \leqslant a \leqslant 0.5p^{1/2}\}$$

for which all solutions to (1) are outside of the interval $[p/4, 3p/4]$, shows the limitations of what can be proven.

References

[1] A. Adolphson, 'On the distribution of angles of Kloosterman sums', *J. Reine Angew. Math.* **395** (1989), 214–220.

[2] W.D. Banks, M.Z. Garaev and I.E. Shparlinski, 'Density of non-residues in short intervals', (preprint 2006).

[3] C.-L. Chai and W.-C.W. Li, 'Character sums, automorphic forms, equidistribution, and Ramanujan graphs. I: The Kloosterman sum conjecture over function fields', *Forum Math.* **15** (2003), 679–699.

[4] W. Duke, J.B. Friedlander and H. Iwaniec, 'Equidistribution of roots of a quadratic congruence to prime moduli', *Ann. of Math.* **141** (1995), 423–441.

[5] É. Fouvry and P. Michel, 'Sommes de modules de sommes d'exponentielles', *Pacific J. Math.* **209** (2003), 261–288.

[6] É. Fouvry and P. Michel, 'Sur le changement de signe des sommes de Kloosterman', *Ann. Math.* (to appear).

[7] H. Iwaniec and E. Kowalski, *Analytic number theory* (American Mathematical Society, Providence, RI, 2004).

[8] N.M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups* (Princeton Univ. Press, Princeton, NJ, 1988).

[9] N.M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy* (Amer. Math. Soc, Providence, RI, 1999).

[10] G. Laumon, 'Exponential sums and l-adic cohomology: A survey', *Israel J. Math.* **120** (2000), 225–257.

[11] R. Lidl and H. Niederreiter, *Finite fields* (Cambridge University Press, Cambridge, 1997).

[12] P. Michel, 'Autour de la conjecture de Sato-Tate pour les sommes de Kloosterman, II', *Duke Math. J.* **92** (1998), 221–254.

[13] P. Michel, 'Minoration de sommes d'exponentielles', *Duke Math. J.* **95** (1998), 227–240.

[14] H. Niederreiter, 'The distribution of values of Kloosterman sums', *Arch. Math.* **56** (1991), 270–277.

[15] P. Sarnak, *Some applications of modular forms* (Cambridge University Press, Cambridge, 1990).

[16] I.E. Shparlinski, 'On the distribution of Kloosterman sums', *Proc. Amer. Math. Soc.* (to appear).

[17] Á. Tóth, 'Roots of quadratic congruences', *Internat. Math. Res. Notices* **2000** (2000), 719–739.

Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
e-mail: igor@ics.mq.edu.au