Michigan Math. J. 56 (2008)

Distribution of Modular Inverses and Multiples of Small Integers and the Sato–Tate Conjecture on Average

IGOR E. SHPARLINSKI

1. Introduction

1.1. Motivation

A rather old conjecture asserts that if $m = p$ is prime then, for any fixed $\varepsilon > 0$ and sufficiently large p, for every integer a there are integers x and y with $|x|, |y| \le p^{1/2+\varepsilon}$ and such that $a \equiv xy \pmod p$; see [14; 16; 17; 18] and references therein. The question has probably been motivated by the following observation. Using the Dirichlet pigeon-hole principle, one can easily show that, for every integer a, there exist integers x and y with $|x|, |y| \le 2p^{1/2}$ and with $a \equiv y/x \pmod p$. Unfortunately, this is known only with $|x|, |y| \ge Cp^{3/4}$ for some absolute constant $C > 0$, which is due to Garaev [15].

On the other hand, it has been shown in the series of works [14; 16; 17; 18] that the congruence $a \equiv xy \pmod p$ is solvable for all but $o(m)$ values of $a = 1, \dots, m-1$, where x and y are significantly smaller than $m^{3/4}$. In particular, it is shown by Garaev and Karatsuba [17] for x and y in the range $1 \le x, y \le m^{1/2}(\log m)^{1+\varepsilon}$. Certainly this result is very sharp. Indeed, it has been observed by Garaev [14] that well-known estimates for integers with a divisor in a given interval immediately imply that, for any $\varepsilon > 0$, almost all residue classes modulo m are *not* of the form $xy \pmod m$ with $1 \le x, y \le m^{1/2}(\log m)^{\kappa-\varepsilon}$, where

$$\kappa = 1 - \frac{1 + \log\log 2}{\log 2} = 0.08607\dots.$$

One can also derive from [10] that, for any $\varepsilon > 0$, the inequality

$$\max\{|x|, |y| : xy \equiv 1 \pmod m\} \ge m^{1/2}(\log m)^{\kappa/2}(\log\log m)^{3/4-\varepsilon}$$

holds:

- for all positive integers $m \le M$, except for possibly $o(M)$ of them;
- for all prime $m = p \le M$, except for possibly $o(M/\log M)$ of them.

Similar questions about the ratios x/y have also been studied; see [14; 17; 28].

Received December 5, 2006. Revision received July 5, 2007.
This work was supported in part by ARC grant DP0556431.

1.2. Our Results

It is clear that these problems are special cases of more general questions about the distribution in small intervals of residues modulo m of ratios a/x and products ax, where $|x| \le X$. In fact, here we consider this for x from more general sets $\mathcal{X} \subseteq [-X, X]$.

Accordingly, for integers a, m, Y, Z and a set of integers $\mathcal{X}$, we denote

$$\begin{aligned} M_{a,m}(\mathcal{X}; Y, Z) = \#\{(x, y) \in \mathcal{X} \times [Z+1, Z+Y] : \\ \gcd(x, m) = 1,\ a/x \equiv y \pmod{m}\}, \\ N_{a,m}(\mathcal{X}; Y, Z) = \#\{(x, y) \in \mathcal{X} \times [Z+1, Z+Y] : ax \equiv y \pmod{m}\}, \end{aligned}$$

where the inversion is always taken modulo m.

We note that although in general the behavior of $N_{a,m}(\mathcal{X}; Y, Z)$ is similar to the behavior of $M_{a,m}(\mathcal{X}; Y, Z)$, there are some substantial differences. For example, if $\mathcal{X} = \{x \in \mathbb{Z} : |x| \le X\}$ for some $X \ge 1$, then $N_{a,m}(\mathcal{X}; X, 0) = 0$ for all integer a with $m - m/X - 1 < a \le m - 1$; see the argument in [14, Sec. 4]. It is also interesting to note that the question of asymptotic behavior of $N_{a,m}(\mathcal{X}; Y, Z)$ has some applications to the discrete logarithm problem; see [29].

Here we extend some of the results of Garaev and Karatsuba [17] and show that if $X, Y \ge m^{1/2+\varepsilon}$ and if $\mathcal{X}$ is a sufficiently massive subset of the interval $[-X, X]$, then $M_{a,m}(\mathcal{X}; Y, Z)$ and $N_{a,m}(\mathcal{X}; Y, Z)$ are close to their expected average values for all but $o(m)$ values of $a = 1, \dots, m$.

It seems that the method of Garaev and Karatsuba [17] is not suitable for obtaining results of this kind. So we use a different approach that is rather similar to the one used in the proof of [5, Thm. 1].

Finally we remark that one can also obtain analogous results for

$$\begin{aligned} &N^*_{a,m}(\mathcal{X}; Y, Z) \\ &\quad = \#\{x \in \mathcal{X} : ax \equiv y \pmod{m},\ \gcd(x, m) = 1,\ y \in [Z+1, Z+Y]\} \end{aligned}$$

and several other similar quantities.

1.3. Applications

For integers r and s and a prime p, we consider Kloosterman sums

$$K_{r,s}(p) = \sum_{n=1}^{p-1} \mathbf{e}_p(rn + sn^{-1}),$$

where $\mathbf{e}_p(z) = \exp(2\pi i z/p)$ and, as before, the inversion is taken modulo p.

For the complex conjugated sum we have

$$\overline{K_{r,s}(p)} = K_{-r,-s}(p) = K_{r,s}(p),$$

so $K_{r,s}(p)$ is real. According to the Weil bound (see [20; 23; 24; 26]), we have

$$|K_{r,s}(p)| \le 2\sqrt{p}, \quad \gcd(r, s, p) = 1.$$

Hence we can now define the angles $\psi_{r,s}(p)$ by the relations

$$K_{r,s}(p) = 2\sqrt{p}\cos\psi_{r,s}(p) \quad \text{and} \quad 0 \le \psi_{r,s}(p) \le \pi.$$

The famous *Sato–Tate* conjecture asserts that, for any fixed nonzero integers r and s, the angles $\psi_{r,s}(p)$ are distributed according to the *Sato–Tate density*

$$\mu_{\mathrm{ST}}(\alpha,\beta) = \frac{2}{\pi}\int_\alpha^\beta \sin^2\gamma\, d\gamma$$

(see [20, Sec. 21.2]). That is, if $\pi_{r,s}(\alpha,\beta;T)$ denotes the number of primes $p \le T$ with $\alpha \le \psi_{r,s}(p) \le \beta$, where as usual $\pi(T)$ denotes the total number of primes $p \le T$, then the Sato–Tate conjecture predicts that

$$\pi_{r,s}(\alpha,\beta;T) \sim \mu_{\mathrm{ST}}(\alpha,\beta)\pi(T), \quad T \to \infty,$$

for all fixed real $0 \le \alpha < \beta \le \pi$; see [20, Sec. 21.2]. It is also known that, if p is sufficiently large and if r and s run independently through $\mathbb{F}_p^*$, then the distribution of $\psi_{r,s}(p)$ is in accordance with the Sato–Tate conjecture [20, Thm. 21.7]. An explicit quantitative bound on the discrepancy between the distribution of $\psi_{r,s}(p)$ for $r, s \in \mathbb{F}_p^*$ and the Sato–Tate distribution is given by Niederreiter [27]. Various modifications and generalizations of this conjecture are given by Katz and Sarnak [23; 24]. Despite a series of significant efforts toward this conjecture, it remains open. See, for example, [1; 7; 11; 12; 23; 24; 25; 27] and references therein.

Here, combining our bounds of $M_{a,m}(\mathcal{X}; Y, Z)$ with a result of Niederreiter [27], we show that on average over r and s and ranging over relatively short intervals $|r| \le R$, $|s| \le S$, the Sato–Tate conjecture holds on average and the sum

$$\Pi_{\alpha,\beta}(R,S,T) = \frac{1}{4RS}\sum_{0<|r|\le R}\ \sum_{0<|s|\le S} \pi_{r,s}(\alpha,\beta;T)$$

satisfies

$$\Pi_{\alpha,\beta}(R,S,T) \sim \mu_{\mathrm{ST}}(\alpha,\beta)\pi(T).$$

Furthermore, over larger intervals, we also estimate the dispersion

$$\Delta_{\alpha,\beta}(R,S,T) = \frac{1}{4RS}\sum_{0<|r|\le R}\ \sum_{0<|s|\le S} (\pi_{r,s}(\alpha,\beta;T) - \mu_{\mathrm{ST}}(\alpha,\beta)\pi(T))^2.$$

We recall that Fouvry and Murty [13] have proved the *Lang–Trotter conjecture* for supersingular primes on average over $|r| \le R$ and $|s| \le S$ for the family of elliptic curves $\mathbb{E}_{r,s}$ given by the *affine Weierstraß equation*:

$$\mathbb{E}_{r,s} : U^2 = V^3 + rV + s.$$

Several more interesting questions on elliptic curves have been studied "on average" for similar families of curves in [3; 4; 6; 8; 9; 19; 21; 22]. However, a similar question for Kloosterman sums has not been addressed.

We note that the technical details of our approach are different from those of Fouvry and Murty [13] (which is based on an application of the Weil bound of exponential sums). For example, their result is nontrivial only if

$$RS \ge T^{3/2+\varepsilon} \quad \text{and} \quad \min\{R,S\} \ge T^{1/2+\varepsilon}$$

for some fixed $\varepsilon > 0$, where the second restriction is related to the range where the Weil bound on incomplete exponential sums with polynomials is nontrivial. The technique of [3] can also be applied to deriving an asymptotic formula for $\Pi_{\alpha,\beta}(R,S,T)$ for the same range of parameters R, S, and T. Apparently it can also be applied to $\Delta_{\alpha,\beta}(R,S,T)$ but certainly in an even narrower range of parameters. On the other hand, our results for $\Pi_{\alpha,\beta}(R,S,T)$ and $\Delta_{\alpha,\beta}(R,S,T)$ are nontrivial for

$$RS \ge T^{1+\varepsilon} \tag{1}$$

and

$$RS \ge T^{2+\varepsilon}, \tag{2}$$

respectively.

We also remark that the results of this work on the behavior of $M_{a,m}(\mathcal{X}; Y, Z)$ on average have been applied in [2] to estimating the number of $\mathrm{SL}_2(\mathbb{F}_p)$ matrices with entries in a given segment $[-T, T]$.

1.4. Notation

Throughout the paper, any implied constants in symbols O and $\ll$ may occasionally depend, where obvious, on the real positive parameter ε and are absolute otherwise. We recall that the expressions $U \ll V$ and $U = O(V)$ are both equivalent to the statement that $|U| \le cV$ holds with some constant $c > 0$.

We also write $o(1)$ for a quantity that tends to zero when the "main" parameter tends to infinity (that is, when $m \to \infty$ in Sections 2.1 and 2.2, $p \to \infty$ in Section 3.1, and $T \to \infty$ in Section 3.2).

We use p, with or without a subscript, to denote a prime number and use m to denote a positive integer. Finally, $\varphi(m)$ denotes, as usual, the Euler function of m.

ACKNOWLEDGMENT. The author wishes to thank Moubariz Garaev for many useful discussions.

2. Congruences

2.1. Inverses

We start with the estimate of the average deviation between $M_{a,m}(\mathcal{X}; Y, Z)$ and its expected value taken over $a = 1, \dots, m$. If the set $\mathcal{X} \subseteq [-X, X]$ is dense enough—for example, if $\#\mathcal{X} \ge X m^{o(1)}$—then this bound is nontrivial for $X, Y \ge m^{1/2+\varepsilon}$ for any fixed $\varepsilon > 0$ and sufficiently large m.

THEOREM 1. *For all positive integers m, X, Y, an arbitrary integer Z, and a set $\mathcal{X} \subseteq \{x \in \mathbb{Z} : |x| \le X\}$,*

$$\sum_{a=1}^{m} \left| M_{a,m}(\mathcal{X}; Y, Z) - \#\mathcal{X}_m \frac{Y}{m} \right|^2 \le \#\mathcal{X}(X+Y)m^{o(1)},$$

where

$$\mathcal{X}_m = \{x \in \mathcal{X} : \gcd(x, m) = 1\}.$$

Proof. Denote

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

Using the identity

$$\frac{1}{m} \sum_{-(m-1)/2 \le h \le m/2} \mathbf{e}_m(hv) = \begin{cases} 1 & \text{if } v \equiv 0 \pmod m, \\ 0 & \text{if } v \not\equiv 0 \pmod m, \end{cases}$$

we write

$$\begin{aligned} M_{a,m}(\mathcal{X}; Y, Z) &= \sum_{x \in \mathcal{X}_m} \sum_{y=Z+1}^{Z+Y} \frac{1}{m} \sum_{-(m-1)/2 \le h \le m/2} \mathbf{e}_m(h(ax^{-1} - y)) \\ &= \frac{1}{m} \sum_{-(m-1)/2 \le h \le m/2} \sum_{x \in \mathcal{X}_m} \mathbf{e}_m(hax^{-1}) \sum_{y=Z+1}^{Z+Y} \mathbf{e}_m(-hy) \\ &= \frac{1}{m} \sum_{-(m-1)/2 \le h \le m/2} \mathbf{e}_m(-hZ) \sum_{\substack{x=1 \\ \gcd(x,m)=1}}^{X} \mathbf{e}_m(hax^{-1}) \sum_{y=1}^{Y} \mathbf{e}_m(-hy). \end{aligned}$$

The term corresponding to $h = 0$ is

$$\frac{1}{m} \sum_{x \in \mathcal{X}_m} \sum_{y=1}^{Y} 1 = \#\mathcal{X}_m \frac{Y}{m}.$$

Hence

$$M_{a,m}(\mathcal{X}; Y, Z) - \#\mathcal{X}_m \frac{Y}{m} \ll \frac{1}{m} E_{a,m}(X, Y),$$

where

$$E_{a,m}(X, Y) = \sum_{1 \le |h| \le m/2} \left| \sum_{x \in \mathcal{X}_m} \mathbf{e}_m(hax^{-1}) \right| \left| \sum_{y=1}^{Y} \mathbf{e}_m(-hy) \right|.$$

Therefore,

$$\sum_{a=1}^{m} \left| M_{a,m}(\mathcal{X}; Y, Z) - \#\mathcal{X}_m \frac{Y}{m} \right|^2 \le \frac{1}{m^2} \sum_{a=1}^{m} E_{a,m}(\mathcal{X}, Y)^2. \tag{3}$$

We now put $J = \lfloor \log(Y/2) \rfloor$ and define the sets

$$\begin{aligned} \mathcal{H}_0 &= \left\{ h \;\middle|\; 1 \le |h| \le \frac{m}{Y} \right\}; \\ \mathcal{H}_j &= \left\{ h \;\middle|\; e^{j-1} \frac{m}{Y} < |h| \le e^j \frac{m}{Y} \right\}, \quad j = 1, \ldots, J; \\ \mathcal{H}_{J+1} &= \left\{ h \;\middle|\; e^J \frac{m}{Y} < |h| \le \frac{m}{2} \right\}. \end{aligned}$$

(We can certainly assume that $J \ge 1$ since otherwise the bound is trivial.)

By the Cauchy inequality we have

$$E_{a,m}(\mathcal{X}, Y)^2 \le (J + 2) \sum_{j=0}^{J+1} E_{a,m,j}(\mathcal{X}, Y)^2, \tag{4}$$

where

$$E_{a,m,j}(\mathcal{X},Y)=\sum_{h\in\mathcal{H}_j}\left|\sum_{x\in\mathcal{X}_m}\mathbf{e}_m(hax^{-1})\right|\left|\sum_{y=1}^{Y}\mathbf{e}_m(-hy)\right|.$$

Using the bound

$$\left|\sum_{y=1}^{Y}\mathbf{e}_m(-hy)\right|=\left|\sum_{y=1}^{Y}\mathbf{e}_m(hy)\right|\ll\min\left\{Y,\frac{m}{|h|}\right\},$$

which holds for any integer h with $0<|h|\le m/2$ (see [20, Bound (8.6)]), we conclude that

$$\sum_{y=1}^{Y}\mathbf{e}_m(-hy)\ll e^{-j}Y,\quad j=0,\dots,J+1.$$

Thus

$$E_{a,m,j}(\mathcal{X},Y)\ll e^{-j}Y\left|\sum_{h\in\mathcal{H}_j}\vartheta_h\sum_{x\in\mathcal{X}_m}\mathbf{e}_m(hax^{-1})\right|,\quad j=0,\dots,J+1,$$

for some complex numbers ϑ_h with $|\vartheta_h|\le 1$ for $|h|\le m/2$. Therefore,

$$\begin{aligned}\sum_{a=1}^{m}E_{a,m,j}(\mathcal{X},Y)^2&\ll e^{-2j}Y^2\sum_{a=1}^{m}\left|\sum_{h\in\mathcal{H}_j}\vartheta_h\sum_{x\in\mathcal{X}_m}\mathbf{e}_m(hax^{-1})\right|^2\\&=e^{-2j}Y^2\sum_{a=1}^{m}\sum_{h_1,h_2\in\mathcal{H}_j}\vartheta_{h_1}\vartheta_{h_2}\sum_{x_1,x_2\in\mathcal{X}_m}\mathbf{e}_m(a(h_1x_1^{-1}-h_2x_2^{-1}))\\&=e^{-2j}Y^2\sum_{h_1,h_2\in\mathcal{H}_j}\vartheta_{h_1}\vartheta_{h_2}\sum_{x_1,x_2\in\mathcal{X}_m}\sum_{a=1}^{m}\mathbf{e}_m(a(h_1x_1^{-1}-h_2x_2^{-1})).\end{aligned}$$

Clearly the inner sum vanishes if $h_1x_1^{-1}\not\equiv h_2x_2^{-1}\pmod m$ and is equal to m otherwise. As a result,

$$\sum_{a=1}^{m}E_{a,m,j}(\mathcal{X},Y)^2\ll e^{-2j}Y^2mT_j,\tag{5}$$

where T_j is the number of solutions to the congruence

$$h_1x_2\equiv h_2x_1\pmod m,\quad h_1,h_2\in\mathcal{H}_j,\ x_1,x_2\in\mathcal{X}_m.$$

We now see that if h_1 and x_2 are fixed then h_2 and x_1 are such that their product $s=h_2x_1\ll e^jmX/Y$ belongs to a prescribed residue class modulo m. Thus there are at most $O(e^jX/Y+1)$ possible values of s and for each fixed $s\ll e^jmX/Y$ there are $m^{o(1)}$ values of h_2 and x_1 with $s=h_2x_1$ (see [30, Sec. I.5.2]). Therefore,

$$T_j\le\#\mathcal{X}\#\mathcal{H}_j\left(\frac{e^jX}{Y}+1\right)m^{o(1)}=\frac{e^{2j}X\#\mathcal{X}m^{1+o(1)}}{Y^2}+\frac{e^j\#\mathcal{X}m^{1+o(1)}}{Y};$$

substitution into (5) then yields

$$\sum_{a=1}^{m}E_{a,m,j}(\mathcal{X},Y)^2\ll e^{-2j}Y^2mT_j=X\#\mathcal{X}m^{2+o(1)}+e^{-j}\#\mathcal{X}Ym^{2+o(1)}.$$

A combination of this bound with (4) yields the inequality

$$\sum_{a=1}^{m} E_{a,m}(\mathcal{X}, Y)^2 \le J^2 X \# \mathcal{X} m^{2+o(1)} + \# \mathcal{X} Y m^{2+o(1)} = \# \mathcal{X}(X+Y) m^{2+o(1)}.$$

Finally, recalling (3), we conclude the proof. □

Corollary 2. *For all positive integers m, X, Y, an arbitrary integer Z, and the set $\mathcal{X} = \{x \in \mathbb{Z} : |x| \le X\}$,*

$$\sum_{a=1}^{m} \left| M_{a,m}(\mathcal{X}; Y, Z) - 2XY \frac{\varphi(m)}{m^2} \right|^2 \le X(X+Y) m^{o(1)}.$$

Proof. Using the Möbius inversion formula involving the Möbius function $\mu(d)$ (see [20, Sec. 1.3] or [30, Sec. I.2.5]), we obtain

$$\sum_{\substack{|x| \le X \\ \gcd(x,m)=1}} 1 = \sum_{d|m} \mu(d) \left(\frac{2X}{d} + O(1) \right) = 2X \sum_{d|m} \frac{\mu(d)}{d} + O\left(\sum_{d|m} |\mu(d)| \right).$$

Using that

$$\sum_{d|m} \frac{\mu(d)}{d} = \frac{\varphi(m)}{m}$$

[30, Sec. I.2.7] and estimating

$$\sum_{d|m} |\mu(d)| \le \sum_{d|m} 1 = m^{o(1)}$$

[30, Sec. I.5.2], we derive

$$\sum_{\substack{|x| \le X \\ \gcd(x,m)=1}} 1 = 2X \frac{\varphi(m)}{m} + O(m^{o(1)}). \tag{6}$$

Substituting (6) in to Theorem 1 concludes the proof. □

From Corollary 2 we may now immediately derive the following.

Corollary 3. *For all positive integers m, X, Y, an arbitrary integer Z, the set $\mathcal{X} = \{x \in \mathbb{Z} : |x| \le X\}$, and an arbitrary real $\Gamma < 1$,*

$$\left| M_{a,m}(\mathcal{X}; Y, Z) - 2XY \frac{\varphi(m)}{m^2} \right| \ge \Gamma \frac{\varphi(m)}{m^2} XY$$

for at most $\Gamma^{-2} Y^{-1} (X^{-1} + Y^{-1}) m^{2+o(1)}$ values of $a = 1, \ldots, m$.

2.2. Multiples

We now estimate the average deviation between $N_{a,m}(\mathcal{X}; Y, Z)$ and its expected value taken over $a = 1, \ldots, m$. Our arguments are almost identical to those of Theorem 1, so we only indicate a few places where they differ (mostly only typographically). As before, if $\mathcal{X} \subseteq [-X, X]$ is dense enough (e.g., if $\#\mathcal{X} \ge X m^{o(1)}$), then this bound is nontrivial for $X, Y \ge m^{1/2+\varepsilon}$ for any fixed $\varepsilon > 0$ and sufficiently large m.

THEOREM 4. *For all positive integers m, X, Y, an arbitrary integer Z, and a set $\mathcal{X} \subseteq \{x \in \mathbb{Z} : |x| \le X\}$,*

$$\sum_{a=1}^{m} \left| N_{a,m}(\mathcal{X}; Y, Z) - \#\mathcal{X}\frac{Y}{m} \right|^2 \le \#\mathcal{X}(X+Y)m^{o(1)}.$$

Proof. As in the proof of Theorem 1, we write

$$N_{a,m}(\mathcal{X}; Y, Z) = \sum_{x\in\mathcal{X}} \sum_{y=Z+1}^{Z+Y} \frac{1}{m} \sum_{-(m-1)/2\le h\le m/2} \mathbf{e}_m(h(ax-y))$$

and obtain, instead of (3), that

$$\sum_{a=1}^{m} \left| N_{a,m}(\mathcal{X}; Y, Z) - \#\mathcal{X}\frac{Y}{m} \right|^2 \le \frac{1}{m^2} \sum_{a=1}^{m} F_{a,m}(\mathcal{X}, Y)^2 + Y^2 m^{-1+o(1)},$$

where

$$F_{a,m}(\mathcal{X}, Y) = \sum_{1<|h|\le m/2} \left| \sum_{x\in\mathcal{X}} \mathbf{e}_m(hax) \right| \left| \sum_{y=1}^{Y} \mathbf{e}_m(-hy) \right|.$$

Furthermore, instead of (4) we obtain

$$F_{a,m}(\mathcal{X}, Y)^2 \le (J+2) \sum_{j=0}^{J+1} F_{a,m,j}(\mathcal{X}, Y)^2,$$

where

$$F_{a,m,j}(\mathcal{X}, Y) = \sum_{h\in\mathcal{H}_j} \left| \sum_{x\in\mathcal{X}} \mathbf{e}_m(hax) \right| \left| \sum_{y=1}^{Y} \mathbf{e}_m(-hy) \right|,$$

with the same sets $\mathcal{H}_j$ as in the proof of Theorem 1. Accordingly, instead of (5) we get

$$\sum_{a=1}^{m} F_{a,m,j}(\mathcal{X}, Y)^2 \ll e^{-2j} Y^2 m V_j,$$

where V_j is the number of solutions to the congruence

$$h_1 x_1 \equiv h_2 x_2 \pmod m, \quad h_1, h_2 \in \mathcal{H}_j,\ x_1, x_2 \in \mathcal{X},\ \gcd(x_1 x_2, m) = 1.$$

Fixing h_1 and x_1 and counting the number of possibilities for the pair (h_2, x_2) as before, we obtain

$$V_j \le \frac{e^{2j} X \#\mathcal{X} m^{1+o(1)}}{Y^2} + \frac{e^j \#\mathcal{X} m^{1+o(1)}}{Y},$$

which yields the desired result. □

Using (6), we deduce an analogue of Corollary 2.

COROLLARY 5. *For all positive integers m, X, Y, an arbitrary integer Z, and the set $\mathcal{X} = \{x \in \mathbb{Z} : |x| \le X\}$,*

$$\sum_{a=1}^{m} \left| N_{a,m}(\mathcal{X}; Y, Z) - 2XY\frac{\varphi(m)}{m^2} \right|^2 \le X(X+Y)m^{o(1)}.$$

Using this corollary, we now immediately derive Corollary 6.

COROLLARY 6. *For all positive integers m, X, Y, an arbitrary integer Z, the set $\mathcal{X} = \{x \in \mathbb{Z} : |x| \le X\}$, and an arbitrary real $\Gamma < 1$,*

$$\left| N_{a,m}(\mathcal{X}; Y, Z) - \frac{2XY}{m} \right| \ge \Gamma \frac{XY}{m}$$

for at most $\Gamma^{-2}Y^{-1}(X^{-1} + Y^{-1})m^{2+o(1)}$ values of $a = 1, \ldots, m$.

3. Distribution of Kloosterman Sums

3.1. Distribution for a Fixed Prime

Let $\mathcal{Q}_{\alpha,\beta}(R, S, p)$ be the set of pairs (r, s) of integers r and s with $|r| \le R$, $|s| \le S$, and $\gcd(rs, p) = 1$ and such that $\alpha \le \psi_{r,s}(p) \le \beta$.

THEOREM 7. *For all primes p and positive integers R and S,*

$$\max_{0 \le \alpha < \beta \le \pi} |\#\mathcal{Q}_{\alpha,\beta}(R, S, p) - 4\mu_{\mathrm{ST}}(\alpha, \beta)RS| \ll RSp^{-1/4} + R^{1/2}S^{1/2}p^{1/2+o(1)}.$$

Proof. Let $\mathcal{A}_p(\alpha, \beta)$ be the set of integers a with $1 \le a \le p-1$ and such that $\alpha \le \psi_{1,a}(p) \le \beta$. By the result of Niederreiter [27], we have:

$$\max_{0 \le \alpha < \beta < \pi} |\#\mathcal{A}_p(\alpha, \beta) - \mu_{\mathrm{ST}}(\alpha, \beta)p| \ll p^{3/4}. \tag{7}$$

Assume that $R \le S$. Then, using that

$$K_{r,s}(p) = K_{1,rs}(p)$$

and defining the set

$$\mathcal{R} = \{r \in \mathbb{Z} : |r| \le R\}, \tag{8}$$

we write

$$\#\mathcal{Q}_{\alpha,\beta}(R, S, p) = \sum_{a \in \mathcal{A}_p(\alpha,\beta)} M_{a,p}(\mathcal{R}; 2S+1, -S-1) + O\left(\frac{RS}{p}\right),$$

where the term $O(RS/p)$ accounts for r and s with $\gcd(rs, p) > 1$. Thus the Cauchy inequality and Theorem 1 yield

$$\begin{aligned}
&\#\mathcal{Q}_{\alpha,\beta}(R,S,p) - \#\mathcal{A}_p(\alpha,\beta)\frac{2R(2S+1)}{p} \\
&\quad \ll \sum_{a\in\mathcal{A}_p(\alpha,\beta)} \left| M_{a,p}(\mathcal{R};2S+1,-S-1) - \frac{2R(2S+1)}{p}\right| + \frac{RS}{p} \\
&\quad \ll \left(p \sum_{a=1}^{p} \left| M_{a,p}(\mathcal{R};2S+1,-S-1) - \frac{2R(2S+1)}{p}\right|^2\right)^{1/2} + \frac{RS}{p} \\
&\quad \ll \sqrt{R(R+S)}\, p^{1/2+o(1)} + \frac{RS}{p}.
\end{aligned}$$

By (7) we see that, for $R \le S$,

$$\#\mathcal{Q}_{\alpha,\beta}(R,S,p) = 4\mu_{\mathrm{ST}}(\alpha,\beta)RS + O(RSp^{-1/4} + R^{1/2}S^{1/2}p^{1/2+o(1)})$$

uniformly over α and β.

For that $R > S$ we write

$$\#\mathcal{Q}_{\alpha,\beta}(R,S,p) = \sum_{a\in\mathcal{A}_p(\alpha,\beta)} M_{a^{-1},p}(\mathcal{S},2R+1,-R-1),$$

where $\mathcal{S} = \{s\in\mathbb{Z} : |s| \le S\}$, and proceed as before. □

3.2. Sato–Tate Conjecture on Average

We start with an asymptotic formula for $\Pi_{\alpha,\beta}(R,S,T)$.

THEOREM 8. *For all positive integers R, S, and T,*

$$\max_{0\le\alpha<\beta\le\pi} |\Pi_{\alpha,\beta}(R,S,T) - \mu_{\mathrm{ST}}(\alpha,\beta)\pi(T)| \ll T^{3/4} + R^{-1/2}S^{-1/2}T^{3/2+o(1)}.$$

Proof. We have

$$\Pi_{\alpha,\beta}(R,S,T) = \frac{1}{4RS}\sum_{p\le T} \#\mathcal{Q}_{\alpha,\beta}(R,S,p).$$

Applying Theorem 7, after simple calculations we obtain the result. □

THEOREM 9. *For all positive integers R, S, and T,*

$$\max_{0\le\alpha<\beta\le\pi} \Delta_{\alpha,\beta}(R,S,T) \ll T^{7/4} + R^{-1/2}S^{-1/2}T^{3+o(1)}.$$

Proof. For two distinct primes p_1 and p_2, let $\mathcal{A}_{p_1p_2}(\alpha,\beta)$ be the set of integers a with $1 \le a \le p_1p_2 - 1$ and such that

$$a \equiv a_1 \pmod{p_1} \quad \text{and} \quad a \equiv a_2 \pmod{p_2}$$

with some $a_1 \in \mathcal{A}_{p_1}(\alpha,\beta)$ and $a_2 \in \mathcal{A}_{p_2}(\alpha,\beta)$.

Then, with the set $\mathcal{R}$ given by (8), we have

$$\sum_{0<|r|\le R}\sum_{0<|s|\le S}\pi_{r,s}(\alpha,\beta;T)^2$$
$$= 2\sum_{p_1<p_2\le T}\left(\sum_{a\in\mathcal{A}_{p_1p_2}(\alpha,\beta)} M_{a,p_1p_2}(\mathcal{R};2S+1,-S-1)+O\left(\frac{RS}{p_1}\right)\right)$$
$$+\,O(RST),$$

where the term $O(RS/p_1)$ accounts for r and s with $\gcd(rs,p_1p_2)>1$ and the term $O(RST)$ accounts for $p_1=p_2$. Therefore,

$$\sum_{0<|r|\le R}\sum_{0<|s|\le S}\pi_{r,s}(\alpha,\beta;T)^2$$
$$= 2\sum_{p_1<p_2\le T}\sum_{a\in\mathcal{A}_{p_1p_2}(\alpha,\beta)} M_{a,p_1p_2}(\mathcal{R};2S+1,-S-1)+O(RST).$$

As in the proof of Theorem 7, we derive

$$\sum_{a\in\mathcal{A}_{p_1p_2}(\alpha,\beta)} M_{a,p_1p_2}(\mathcal{R};2S+1,-S-1)$$
$$= 4\#\mathcal{A}_{p_1p_2}(\alpha,\beta)\frac{RS}{p_1p_2}+O\left(\sqrt{RS}(p_1p_2)^{1/2+o(1)}\right).$$

Thus, using (7) yields

$$\sum_{a\in\mathcal{A}_{p_1p_2}(\alpha,\beta)} M_{a,p_1p_2}(\mathcal{R};2S+1,-S-1)$$
$$= 4\mu_{\mathrm{ST}}(\alpha,\beta)^2RS+O\left(RSp_1^{-1/4}+\sqrt{RS}(p_1p_2)^{1/2+o(1)}\right).$$

Hence,

$$\sum_{0<|r|\le R}\sum_{0<|s|\le S}\pi_{r,s}(\alpha,\beta;T)^2$$
$$= 8\mu_{\mathrm{ST}}(\alpha,\beta)^2RS\sum_{p_1<p_2\le T}1+O\left(RST^{7/4}+\sqrt{RS}T^{3+o(1)}\right)$$
$$= 4\mu_{\mathrm{ST}}(\alpha,\beta)^2RS\pi(T)^2+O\left(RST^{7/4}+\sqrt{RS}T^{3+o(1)}\right).$$

Combining this bound with Theorem 8 then shows the desired result. □

Clearly, Theorems 8 and 9 are nontrivial under the conditions (1) and (2), respectively. We also remark that, by combining [12, Lemma 4.4] (taken with $r=1$) together with the method of [27], one can prove an asymptotic formula for $\#\mathcal{Q}_{\alpha,\beta}(1,S,p)$ when $S\ge p^{3/4+\varepsilon}$ for any fixed $\varepsilon>0$. In turn, this leads to an asymptotic formula for $\Pi_{\alpha,\beta}(1,S,T)$ in the same range $S\ge T^{3/4+\varepsilon}$. However, it is not clear how to estimate $\Delta_{\alpha,\beta}(R,S,T)$ within this approach.

References

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

[2] O. Ahmadi and I. E. Shparlinski, *Distribution of matrices with restricted entries over finite fields,* preprint, 2006.

[3] A. Akbary, C. David, and R. Juricevic, *Average distributions and products of special values of L-series,* Acta Arith. 111 (2004), 239–268.

[4] S. Baier, *The Lang–Trotter conjecture on average,* preprint, 2006.

[5] W. D. Banks, R. Heath-Brown, and I. E. Shparlinski, *On the average value of divisor sums in arithmetic progressions,* Internat. Math. Res. Notices 2005 (2005), 1–25.

[6] J. Battista, J. Bayless, D. Ivanov, and K. James, *Average Frobenius distributions for elliptic curves with nontrivial rational torsion,* Acta Arith. 119 (2005), 81–91.

[7] 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.

[8] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves,* Internat. Math. Res. Notices 1999 (1999), 165–183.

[9] ———, *Average Frobenius distribution for inerts in* $\mathbb{Q}(i)$, J. Ramanujan Math. Soc. 19 (2004), 181–201.

[10] K. Ford, M. R. Khan, I. E. Shparlinski, and C. L. Yankov, *On the maximal difference between an element and its inverse in residue rings,* Proc. Amer. Math. Soc. 133 (2005), 3463–3468.

[11] É. Fouvry and P. Michel, *Sur le changement de signe des sommes de Kloosterman,* Ann. of Math. (2) 165 (2007), 675–715.

[12] É. Fouvry, P. Michel, J. Rivat, and A. Sárközy, *On the pseudorandomness of the signs of Kloosterman sums,* J. Austral. Math. Soc. 77 (2004), 425–436.

[13] É. Fouvry and M. R. Murty, *On the distribution of supersingular primes,* Canad. J. Math. 48 (1996), 81–104.

[14] M. Z. Garaev, *Character sums in short intervals and the multiplication table modulo a large prime,* Monatsh. Math. 148 (2006), 127–138.

[15] ———, *On the logarithmic factor in error term estimates in certain additive congruence problems,* Acta Arith. 124 (2006), 27–39.

[16] M. Z. Garaev and A. A. Karatsuba, *On character sums and the exceptional set of a congruence problem,* J. Number Theory 114 (2005), 182–192.

[17] ———, *The representation of residue classes by products of small integers,* Proc. Edinburgh Math. Soc. (2) 50 (2007), 363–375.

[18] M. Z. Garaev and K.-L. Kueh, *Distribution of special sequences modulo a large prime,* Internat. J. Math. Math. Sci. 50 (2003), 3189–3194.

[19] E.-U. Gekeler, *Frobenius distributions of elliptic curves over finite prime fields,* Internat. Math. Res. Notes 2003 (2003), 1999–2018.

[20] H. Iwaniec and E. Kowalski, *Analytic number theory,* Amer. Math. Soc. Colloq. Publ., 53, Amer. Math. Soc., Providence, RI, 2004.

[21] K. James, *Average Frobenius distributions for elliptic curves with 3-torsion,* J. Number Theory 109 (2004), 278–298.

[22] K. James and G. Yu, *Average Frobenius distribution of elliptic curves,* Acta Arith. 124 (2006), 79–100.

[23] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups,* Ann. of Math. Stud., 116, Princeton Univ. Press, Princeton, NJ, 1988.

[24] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy,* Amer. Math. Soc. Colloq. Publ., 45, Amer. Math. Soc, Providence, RI, 1999.

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

[26] R. Lidl and H. Niederreiter, *Finite fields,* Encyclopedia Math. Appl., 20, Cambridge Univ. Press, Cambridge, 1997.

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

[28] I. A. Semaev, *On the number of small solutions of a linear homogeneous congruence,* Mat. Zametki 50 (1991), 102–107 (in Russian).

[29] ———, *An algorithm for evaluation of discrete logarithms in some nonprime finite fields,* Math. Comp. 67 (1998), 1679–1689.

[30] G. Tenenbaum, *Introduction to analytic and probabilistic number theory,* Cambridge Stud. Adv. Math., 46, Cambridge Univ. Press, Cambridge, 1995.

Department of Computing
Macquarie University
Sydney, NSW 2109
Australia

igor@ics.mq.edu.au