Size of product of a number and its multiplicative inverse, 
Moments of L-functions and Exponential Sums

Tsz Ho Chan

December 30, 2014

Abstract

In this paper, we study the average size of the product of a number and its multiplicative inverse modulo a prime $p$. This turns out to be related to moments of L-functions and leads to a curious asymptotic formula for a certain triple exponential sum.

1 Introduction and main results

Let $p$ be a prime number. For any $(a, p) = 1$, let $\overline{a}$ be the positive integer less than $p$ such that $a\overline{a} \equiv 1 \pmod{p}$. Of course $a\overline{a}$ can be as small as 1 for $a = 1$ and as big as $(p - 1)^2$ for $a = p - 1$. So one can ask on average how big $a\overline{a}$ is. This leads us to study

$$S := \sum_{a=1}^{p-1} a\overline{a} = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} ab \quad \text{such that } ab \equiv 1 \pmod{p}. \quad (1)$$

More generally, one defines

$$S(d) := \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} ab \quad \text{such that } ab \equiv d \pmod{p}. \quad (2)$$

We have

Theorem 1 For $(d, p) = 1$,

$$\sum_{a=1}^{p-1} \sum_{b=1}^{p-1} ab = \frac{p^3}{4} + O(p^{5/2} \log^2 p).$$

For a Dirichlet character $\chi$, let $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ be the corresponding Dirichlet $L$-function which has meromorphic continuation over the entire complex plane. And as a by-product of the proof of Theorem 1, we have

Corollary 1 For $(d, p) = 1$,

$$\sum_{\chi \neq \chi_0} \chi(d)L(0, \chi)^2 \ll p^{3/2} \log^2 p.$$ 

One can ask how good the error term in Theorem 1 is. To this we consider the mean square error and have
Theorem 2 For prime $p$,
\[
\left| \sum_{d=1}^{p-1} \left( S(d) - \frac{p^2(p-1)}{4} \right) \right|^2 = \frac{5}{144} \frac{p^2(p^2 - 1)^3}{(p^2 + 1)} + O\left( p^\delta \log p \right),
\]
This tells us that for some $1 \leq d \leq p - 1$, we have
\[
\left| S(d) - \frac{p^2(p-1)}{4} \right| \gg p^{5/2}.
\]
So the error term in Theorem 1 is sharp apart from the logarithmic factor.

One can consider higher dimensional analogue of (2) by defining
\[
S_k(d) := \sum_{a_1=1}^{p-1} \sum_{a_k=1}^{p-1} \cdots \sum_{a_{k-1}=1}^{p-1} a_1 a_2 \cdots a_k \quad (a_1 a_2 \cdots a_k \equiv d \pmod{p})
\]
and one can prove

Theorem 3 For $k \geq 3$ and $(d, p) = 1$,
\[
S_k(d) = \frac{p^k(p-1)^{k-1}}{2^k} + O_k(p^{3k/2} \log p^k).
\]
When $k = 3$, one can do slightly better by exponential sum method and get

Theorem 4 For $(d, p) = 1$,
\[
S_3(d) = \frac{p^5}{8} + O_k(p^{9/2} \log p^2).
\]
This improvement on the error term may not be very worth doing. But as a by-product of its proof, we have an interesting result on a triple exponential sum, namely

Theorem 5 For $(l, p) = 1$,
\[
\sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} abc e\left( \frac{labc}{p} \right) = -\frac{p^5}{8} + O(p^{9/2} \log^3 p).
\]
We will leave the interested readers to derive similar results for exponential sums with more variables.

**Some Notations** Throughout the paper, the symbol $\overline{a}$ stands for the multiplicative inverse of $a \pmod{q}$ (i.e. $a \overline{a} \equiv 1 \pmod{q}$). The notations $f(x) = O(g(x))$, $f(x) \ll g(x)$ and $g(x) \gg f(x)$ are all equivalent to $|f(x)| \leq Cg(x)$ for some constant $C > 0$. Finally $f(x) = O_\lambda(g(x))$, $f(x) \ll_\lambda g(x)$ or $g(x) \gg_\lambda f(x)$ mean that the implicit constant $C$ may depend on $\lambda$.

## 2 Some Lemmas

**Lemma 1** For $z \neq 1$ and $z^p = 1$, \[
\sum_{b=1}^{p-1} b z^b = \frac{-p}{1-z}.
\]

Proof: As $1 + z + z^2 + \cdots + z^{p-1} = 0$, one can check directly that
\[
\left( \sum_{b=1}^{p-1} b z^b \right) (1 - z) = z + z^2 + \cdots + z^{p-1} - (p - 1) z^p = -1 - (p - 1) = -p
\]
which gives the lemma after dividing by $1 - z$. 

2
Lemma 2 For \( z \neq 1 \) and \( z^p = 1 \), \( \sum_{b=1}^{p-1} \frac{1}{1 - z^b} = \frac{p-1}{2} \).

Proof: Notice that \( \frac{1}{1-z} + \frac{1}{1-z^p} = \frac{1}{1-z^p} + \frac{z^p}{1-z^p} = 1 \) as \( |z| = 1 \). Therefore
\[
\sum_{b=1}^{p-1} \frac{1}{1 - z^b} = \frac{1}{2} \sum_{b=1}^{p-1} \left( \frac{1}{1 - z^b} + \frac{1}{1 - z^{p-b}} \right) = \frac{1}{2} \sum_{b=1}^{p-1} 1 = \frac{p-1}{2}.
\]

Lemma 3 For \( z \neq 1 \), \( z^p = 1 \) and \( 1 \leq d < p \), \( \sum_{b=1}^{p-1} \frac{z^{-db}}{1 - z^b} = \frac{p-1}{2} - d \).

Proof: Consider
\[
\sum_{b=1}^{p-1} \frac{1 - z^{-db}}{1 - z^b} = \sum_{b=1}^{p-1} \frac{-z^{-db}(1 - z^{db})}{1 - z^b} = -\sum_{b=1}^{p-1} z^{-db} \sum_{j=0}^{d-1} z^{jb}.
\]
Therefore by Lemma 2,
\[
d = \sum_{b=1}^{p-1} \frac{1}{1 - z^b} - \sum_{b=1}^{p-1} \frac{z^{-db}}{1 - z^b} = \frac{p-1}{2} - \sum_{b=1}^{p-1} \frac{z^{-db}}{1 - z^b}
\]
which gives the lemma after rearranging terms.

Lemma 4 For prime \( p \) and \( (k, p) = 1 \),
\[
\sum_{a=1}^{p-1} a e\left(\frac{ka}{p}\right) \ll p^{3/2} \log p.
\]

Proof: By Weil bound on incomplete Kloosterman sum, we have
\[
F(u) := \sum_{a=1}^{u} e\left(\frac{ka}{p}\right) \ll p^{1/2} \log p
\]
for \( 1 \leq u < p \). Using this and partial summation,
\[
\sum_{a=1}^{p-1} a e\left(\frac{ka}{p}\right) = \int_{1-}^{p-1} u dF(u) = (p-1)F(p-1) - \int_{1-}^{p-1} F(u) du \ll p^{3/2} \log p.
\]

Lemma 5 For \( p > 1 \),
\[
\sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \ll p \log p.
\]

Proof: Observe that \( |1 - e(-k/p)| \geq |\text{Im}(1 - e(-k/p))| = |\sin 2k\pi/p| \). For \( 0 \leq k < p/4 \), \( |\sin 2k\pi/p| \geq k/p \) by observing that the sine function is above the line \( y = 2x/\pi \) for \( 0 \leq x \leq \pi/2 \). So
\[
\sum_{k<p/4} |1 - e(-k/p)| \leq \sum_{k<p/4} \frac{1}{k/p} \ll p \log p.
\]
Using \( \sin(\pi - x) = \sin x \), we have

\[
\sum_{p/4 < k \leq p/2} \frac{1}{|1 - e(-k/p)|} \ll p \log p.
\]

Hence

\[
P \sum_{k=1}^{p/2} \frac{1}{|1 - e(-k/p)|} \ll p \log p + 1 \ll p \log p
\]  \hspace{1cm} (3)

where the 1 may come from the term when \( k = p/4 \). By complex conjugation,

\[
\frac{1}{|1 - e(-k/p)|} = \frac{1}{|1 - e(-(p-k)/p)|}.
\]

So from (3),

\[
P - 1 \sum_{k=p/2}^{p-1} \frac{1}{|1 - e(-k/p)|} \ll p \log p
\]  \hspace{1cm} (4)

and the lemma follows from (3) and (4).

### 3 Proof of Theorems 1 and 3 and Corollary 1

**Proof of Theorem 1** We use exponential sum to study (2). By orthogonality of additive characters,

\[
S(d) = \frac{1}{p} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} ab \sum_{k=1}^{p} e \left( \frac{k(d-a)b}{p} \right) = \frac{p(p-1)^2}{4} + \frac{1}{p} \sum_{k=1}^{p-1} \sum_{a=1}^{p-1} ae \left( \frac{kd}{p} \right) \sum_{b=1}^{p-1} be \left( \frac{-kb}{p} \right)
\]

where \( e(u) = e^{2\pi i u} \). Hence, by Lemma 1

\[
S(d) = \frac{p(p-1)^2}{4} - \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{a=1}^{p-1} ae \left( \frac{kd}{p} \right).
\]  \hspace{1cm} (5)

By Lemmas 4 and 5

\[
S(d) = \frac{p(p-1)^2}{4} + O \left( p^{3/2} \log p \sum_{k=1}^{p-1} \frac{1}{|1 - e(-k/p)|} \right) = \frac{p^3}{4} + O(p^{5/2} \log^2 p).
\]  \hspace{1cm} (6)

**Proof of Corollary 1** Another way to study (2) is through character sums. By orthogonality of Dirichlet characters, we have

\[
S(d) = \frac{1}{\phi(p)} \sum_{\chi \mod p} \chi(d) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} ab \chi(a) \chi(b)
\]

\[
= \frac{1}{p-1} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} ab + \frac{1}{\phi(p)} \sum_{\chi \neq \chi_0} \chi(d) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} ab \chi(a) \chi(b)
\]

\[
= \frac{p^2(p-1)}{4} + \frac{1}{p-1} \sum_{\chi \neq \chi_0} \chi(d) \left( \sum_{a=1}^{p-1} a \chi(a) \right)^2.
\]

4
As \( \sum_{a \pmod p} a \chi(a) = -pL(0, \chi) \) (see [1] page 310) and combine with the functional equation for Dirichlet \( L \)-functions, we have
\[
S(d) = \frac{p^2(p-1)}{4} + \frac{p^2}{p-1} \sum_{\chi \neq \chi_0} \chi(d)L(0, \chi)^2.
\] (7)

Comparing (7) and (6), we have
\[
\sum_{\chi \neq \chi_0} \chi(d)L(0, \chi)^2 \ll p^{3/2} \log^2 p.
\]

**Proof of Theorem 3** The character sum method can be used to study higher dimension analogue of Theorem 1. By orthogonality of Dirichlet characters, we have
\[
S_k(d) = \frac{1}{\varphi(p)} \sum_{\chi \pmod p} \chi(d) \sum_{a_1=1}^{p-1} \sum_{a_2=1}^{p-1} \ldots \sum_{a_k=1}^{p-1} a_1 a_2 \ldots a_k \chi(a_1) \chi(a_2) \ldots \chi(a_k)
\]
\[
= \frac{1}{p-1} \sum_{a_1=1}^{p-1} \sum_{a_2=1}^{p-1} \ldots \sum_{a_k=1}^{p-1} a_1 a_2 \ldots a_k + \frac{1}{\varphi(p)} \sum_{\chi \neq \chi_0} \chi(d) \sum_{a_1=1}^{p-1} \sum_{a_2=1}^{p-1} \ldots \sum_{a_k=1}^{p-1} a_1 a_2 \ldots a_k \chi(a_1) \chi(a_2) \ldots \chi(a_k)
\]
\[
= \frac{p^k(p-1)^{k-1}}{2^k} + \frac{1}{p-1} \sum_{\chi \neq \chi_0} \chi(d) \left( \sum_{a=1}^{p-1} \chi(a) \right)^k.
\]

As \( \sum_{a \pmod p} a \chi(a) \ll p^{3/2} \log p \) by Polya-Vinogradov inequality and partial summation, we have
\[
S_k(d) = \frac{p^k(p-1)^{k-1}}{2^k} + O_k(p^{3k/2} \log^k p)
\]
which gives Theorem 3

### 4 Proof of Theorem 2

Define
\[
M := \sum_{d=1}^{p-1} |S(d) - \frac{p^2(p-1)}{4}|^2.
\]

By (7),
\[
M = \sum_{d=1}^{p-1} \left| \frac{p^2}{p-1} \sum_{\chi \neq \chi_0} \chi(d)L(0, \chi)^2 \right|^2
\]
\[
= \frac{p^4}{(p-1)^2} \sum_{\chi_1 \neq \chi_0} \sum_{\chi_2 \neq \chi_0} L(0, \chi_1)^2 L(0, \chi_2)^2 \sum_{d=1}^{p-1} \overline{\chi_1(d)} \chi_2(d)
\]
\[
= \frac{p^4}{(p-1)} \sum_{\chi_1 \neq \chi_0} |L(0, \chi_1)|^4 = \frac{p^4}{(p-1)} \sum_{\chi_1 \pmod p} |L(0, \chi_1)|^4
\]
by orthogonality of Dirichlet characters and \( L(0, \chi) = 0 \) when \( \chi(-1) = 1 \). Now by \( L(0, \chi) = \frac{\tau(\chi)}{\pi i} L(1, \chi) \) and \( |\tau(\chi)| = p^{1/2} \),
\[
M = \frac{p^6}{\pi^4(p-1)} \sum_{\chi_1 \pmod p} |L(1, \chi_1)|^4 = \frac{5}{144} \frac{p^2(p^2-1)^3}{(p^2+1)} + O(p^{5.3 \log p / \log \log p})
\]
by Lemma 2 of Zhang \[2\]. This tells us that for some $1 \leq d \leq p - 1$, we have

$$|S(d) - \frac{p^2(p - 1)}{4}| \gg p^{5/2}.$$ 

So the error term in (\ref{eq:5}) is sharp apart from the logarithmic factor.

5 Double exponential sum

In this section, we want to study

$$D := \sum_{a=1}^{p-1} \sum_{k=1}^{p-1} ab \ e\left(\frac{lab}{p}\right).$$

(8)

First, observe that

$$D = \sum_{d=1}^{p-1} e\left(\frac{ld}{p}\right) \ \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} ab \equiv d \ (\text{mod } p).$$

By (\ref{eq:5}),

$$D = -\frac{p(p - 1)^2}{4} - \sum_{d=1}^{p-1} e\left(\frac{ld}{p}\right) \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{a=1}^{p-1} e\left(\frac{kda}{p}\right).$$

Now the sums above can be rewritten as

$$= -\sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{a=1}^{p-1} a \sum_{d=1}^{p-1} e\left(\frac{d(l + k\bar{a})}{p}\right)$$

$$-\frac{p(p - 1)^2}{4} + p \sum_{a=1}^{p-1} \frac{a}{1 - e(al/p)}$$

by Lemma 2. Therefore

$$D = -p \sum_{a=1}^{p-1} \frac{a}{1 - e(al/p)}.$$ 

(9)

6 Triple exponential sum: Proof of Theorem \[5\]

In this section, we study

$$T := \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} abc \ e\left(\frac{lab}{p}\right)$$

where $0 < l < p$. One can rearrange it as

$$T = \sum_{c=1}^{p-1} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} ab \ e\left(\frac{lca}{p}\right) = -p \sum_{c=1}^{p-1} \sum_{a=1}^{p-1} \frac{a}{1 - e(al/p)}$$
by \((\ref{lem:grouping})\). Grouping the sums according to \(ac \equiv d \pmod{p}\), we have

\[
T = -p \sum_{d=1}^{p-1} \frac{1}{1 - e(dl/p)} \sum_{a=1}^{p-1} \sum_{c=1}^{p-1} ac.
\]

By \((\ref{eq:term})\),

\[
T = -p \sum_{d=1}^{p-1} \frac{1}{1 - e(dl/p)} \left[ \frac{p(p-1)^2}{4} - \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{a=1}^{p-1} ae \left( \frac{k\overline{ac}}{p} \right) \right]
\]

\[
= \frac{p^2(p-1)^3}{8} + p \sum_{d=1}^{p-1} \frac{1}{1 - e(dl/p)} \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{a=1}^{p-1} ae \left( \frac{k\overline{ac}}{p} \right)
\]  

by Lemma \((\ref{lem:term})\) Theorem \((\ref{thm:main})\) follows by observing that the above has a main term \(-p^3/8\) and an error term \(O(p^{3/2} \log^3 p)\) by Lemmas \((\ref{lem:grouping})\) and \((\ref{lem:term})\).

### 7 Proof of Theorem \((\ref{thm:main})\)

Now we are ready to study

\[
S_3(d) = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} abc \pmod{d}.
\]

By orthogonality of additive characters,

\[
S_3(d) = \frac{1}{p} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} abc \sum_{l=1}^{p-1} e \left( \frac{l(abc - d)}{p} \right) = \frac{p^2(p-1)^3}{8} + \frac{1}{p} \sum_{l=1}^{p-1} e \left( -\frac{dl}{p} \right) \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} abc \sum_{l=1}^{p-1} e \left( \frac{labc}{p} \right).
\]

By \((\ref{eq:term})\),

\[
S_3(d) = \frac{p^2(p-1)^3}{8} + \sum_{l=1}^{p-1} e \left( -\frac{dl}{p} \right) \left[ \frac{p(p-1)^3}{8} + \sum_{l=1}^{p-1} \frac{1}{1 - e(ltl/p)} \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{a=1}^{p-1} ae \left( \frac{k\overline{ac}}{p} \right) \right]
\]

\[
= \frac{p(p+1)(p-1)^3}{8} + \sum_{l=1}^{p-1} \left( -\frac{p-1}{2} - t\overline{d} \right) \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{a=1}^{p-1} ae \left( \frac{k\overline{ac}}{p} \right) =: S_1 + S_2
\]

by Lemma \((\ref{lem:orthogonality})\) Now

\[
S_2 = \frac{p-1}{2} \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{a=1}^{p-1} a \sum_{l=1}^{p-1} e \left( \frac{kl\overline{ac}}{p} \right) + \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{t=1}^{p-1} t \sum_{a=1}^{p-1} ae \left( \frac{k\overline{ac}}{p} \right)
\]

\[
= -\frac{p-1}{2} \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{a=1}^{p-1} a + \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{t=1}^{p-1} t \sum_{a=1}^{p-1} ae \left( \frac{k\overline{ac}}{p} \right)
\]

\[
= -\frac{p(p-1)^3}{8} + \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{t=1}^{p-1} \sum_{a=1}^{p-1} ate \left( \frac{kt\overline{ac}}{p} \right)
\]
\[
\sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{c=1}^{p-1} \sum_{t=1}^{p-1} e \left( \frac{kt^c}{p} \right) \sum_{a \equiv c \pmod{p}}^{p-1} a.
\]

By (5),

\[
S_2 = - \frac{p(p-1)^3}{8} + \sum_{k=1}^{p-1} \frac{1}{1 - e(-k/p)} \sum_{c=1}^{p-1} e \left( \frac{kd}{p} \right) \sum_{l=1}^{p-1} \frac{1}{1 - e(-l/p)} \sum_{a=1}^{p-1} e \left( \frac{ln}{p} \right)
\]

where \( S(a, b; p) \) is the Kloosterman sum. Using Weil's bound on Kloosterman sum and Lemma \( \text{Lemma 5} \) we have

\[
S_2 = - \frac{p(p-1)^3}{4} + O(p^{9/2} \log^2 p).
\]

Consequently,

\[
S_3(d) = \frac{p(p-1)^4}{8} + O(p^{9/2} \log^2 p)
\]

which gives Theorem 4.

References

[1] H. L. Montgomery and R. C. Vaughan, Multiplicative Number Theory. Classical Theory, Cambridge University Press, 2007.

[2] W. Zhang, A Sum Analogous to the Dedekind Sums and its Mean Value Formula, J. Number Theory (1) 89 (2001), 1–13.

White Station High School
514 S. Perkins Road,
Memphis, TN 38117
U.S.A.