DISTRIBUTION OF DIFFERENCE BETWEEN INVERSES OF CONSECUTIVE INTEGERS MODULO P

Tsz Ho Chan

Department of Mathematics, Case Western Reserve University, Cleveland, OH 44106, USA

txc50@cwru.edu

Received: 11/19/03, Revised: 2/9/04, Accepted: 3/24/04, Published: 3/25/04

Abstract

Let $p > 2$ be a prime number. For each integer $0 < n < p$, define $\overline{n}$ by the congruence $n\overline{n} \equiv 1 \pmod{p}$ with $0 < \overline{n} < p$. We are led to study the distribution behavior of $\overline{n} - \overline{n+1}$ in order to prove the asymptotic formula

$$\sum_{n=1}^{p-2} |\overline{n} - \overline{n+1}| = \frac{1}{3}p^2 + O(p^{3/2}\log^3 p).$$

1. Introduction

For any prime p and any integer $0 < n < p$, there is one and only one $\overline{n}$ with $0 < \overline{n} < p$ satisfying $n\overline{n} \equiv 1 \pmod{p}$. We are interested in how the inverses $\overline{n}$ fluctuate as n runs from 1 to $p-1$. In particular, we look at the sum

$$S_p = \sum_{n=1}^{p-2} |\overline{n} - \overline{n+1}| \tag{1}$$

For any integer k, one can easily show that there are at most 2 solutions to the congruence equation $\overline{n} - \overline{n+1} \equiv k \pmod{p}$. From this, we have

$$\frac{1}{8}p^2 - \frac{1}{2}p \le \sum_{n=1}^{[p/4]} 4k \le S_p \le \sum_{n=p-[p/4]-2}^{p-2} 4k \le \frac{7}{8}p^2 + \frac{7}{2}p$$

where $[x]$ denotes the greatest integer $\le x$. So, S_p has order p^2 and the natural question is whether $\lim_{p\to\infty} S_p/p^2$ exists. To this, we have the following.

Theorem 1. *For any prime $p > 2$,*

$$S_p = \sum_{n=1}^{p-2} |\overline{n} - \overline{n+1}| = \frac{1}{3}p^2 + O(p^{3/2}\log^3 p).$$

Hence, on average, the difference between inverses of consecutive integers, $|\overline{n} - \overline{n+1}|$, is about $p/3$. More generally, we have the following result.

Theorem 2. *For any prime $p > 2$ and $\lambda > 0$,*

$$\sum_{n=1}^{p-2} |\overline{n} - \overline{n+1}|^{\lambda} = \frac{2}{(\lambda+1)(\lambda+2)}p^{\lambda+1} + O(p^{\lambda+1/2}\log^3 p).$$

To prove Theorem 1 or 2, we are led to study

$$T_+(p,k) = \#\{n : 0 < n < p, 0 < \overline{n} - \overline{n+1} \le k\},$$
$$T_-(p,k) = \#\{n : 0 < n < p, -k \le \overline{n} - \overline{n+1} < 0\}, \text{ and}$$
$$T(p,k) = T_+(p,k) + T_-(p,k) = \#\{n : 0 < n < p, 0 < |\overline{n} - \overline{n+1}| \le k\}$$

for integer $0 < k < p$. We have

Theorem 3. *For any prime $p > 2$ and any integer $0 < k < p$,*

$$T_{\pm}(p,k) = k - \frac{k^2}{2p} + O(p^{1/2}\log^3 p).$$

Our method of proof is motivated by Professor W.P. Zhang's paper [5] involving Kloosterman sums and trigonometric sums. The proofs of Theorems 1, 2 and 3 extend to pairs $\overline{n}$ and $\overline{n+l}$ for fixed integer $l \not\equiv 0 \pmod p$ with slight modifications.

2. Exponential and Kloosterman sums

First, we start with some notation. Letting $e(y) = e^{2\pi i y}$, we denote the Kloosterman sum

$$S(m,n;q) := \sum_{\substack{d \pmod q \\ (d,q)=1}} e\Big(\frac{md + n\overline{d}}{q}\Big).$$

Lemma 1. *Let p be a prime number. For any integer a and $b \not\equiv 0 \pmod p$,*

$$\sum_{x=1}^{p}{}' e\Big(\frac{\frac{ax+b}{x(x\pm1)}}{p}\Big) \ll p^{1/2}$$

where $\sum'$ is over all $x \pmod p$ except the roots of $x(x \pm 1)$ in F_p.

Proof. It follows from the Bombieri-Weil bound [1] for exponential sums in the form by Moreno and Moreno [4, Theorem 2] provided that $\frac{ax+b}{x(x\pm1)}$ is not of the form $h(x)^p - h(x)$ with $h(x) \in \overline{F}_p$, where $\overline{F}_p$ is the algebraic closure of F_p. This is true in our situation. For otherwise, say

$$\frac{ax+b}{x(x\pm1)} = \Big(\frac{F(x)}{G(x)}\Big)^p - \frac{F(x)}{G(x)}$$

with $F(x)$ and $G(x)$ polynomials over $\overline{F}_p$ such that $(F(x), G(x)) = 1$. Then

$$(ax+b)G(x)^p = x(x\pm1)F(x)(F(x)^{p-1} - G(x)^{p-1}). \tag{2}$$

Since $F(x)$ and $G(x)$ are relatively prime, we have $G(x)^p | x(x\pm1)$. This forces $G(x)$ to be a nonzero constant polynomial. Contradiction occurs if one compares the degrees in (2). □

Lemma 2. *Let $p > 2$ be a prime number. For any integers r and s,*

$$\sum_{n=1}^{p-1} e\Big(\frac{\pm n}{p}\Big) S(r,n;p)\overline{S(s,n;p)} \ll p^{3/2}. \tag{3}$$

Here $\overline{S(s,n;p)}$ stands for the complex conjugate of $S(s,n;p)$.

Proof.

1. $r \equiv 0 \pmod p$. Then $S(r,n;p) = -1$ for $1 \le n \le p-1$. So, the left side of (3) is

$$\begin{aligned} &= \sum_{n=1}^{p-1} e\Big(\frac{\pm n}{p}\Big) \sum_{d=1}^{p-1} e\Big(\frac{-sd - n\overline{d}}{p}\Big) \\ &= \sum_{d=1}^{p-1} e\Big(\frac{-sd}{p}\Big) \sum_{n=1}^{p-1} e\Big(\frac{-n(\overline{d} \mp 1)}{p}\Big) \ll \sum_{\substack{d=1 \\ \overline{d} \not\equiv \pm 1 (p)}}^{p-1} 1 + p \ll p. \end{aligned}$$

2. $s \equiv 0 \pmod p$. Similar to case 1.

3. $r \not\equiv s \pmod p$ and $(r,p) = 1 = (s,p)$. The left hand side of (3)

$$\begin{aligned}
&= \sum_{n=1}^{p-1} e\Big(\frac{\pm n}{p}\Big) \sum_{a=1}^{p-1} e\Big(\frac{ra + n\overline{a}}{p}\Big) \sum_{b=1}^{p-1} e\Big(\frac{-sb - n\overline{b}}{p}\Big) \\
&= \sum_{a=1}^{p-1}\sum_{b=1}^{p-1} e\Big(\frac{ra - sb}{p}\Big) \sum_{n=1}^{p-1} e\Big(\frac{(\overline{a} - \overline{b} \pm 1)n}{p}\Big) \\
&= \sum_{c=1}^{p-1}\sum_{d=1}^{p-1} e\Big(\frac{r\overline{c} - s\overline{d}}{p}\Big) \sum_{n=1}^{p-1} e\Big(\frac{(c - d \pm 1)n}{p}\Big) \\
&= (p-1)\sum_{d=1}^{p}{}' e\Big(\frac{r\overline{d \mp 1} - s\overline{d}}{p}\Big) - \sum_{\substack{c=1 \\ c\neq d\mp 1}}^{p-1}\sum_{d=1}^{p-1} e\Big(\frac{r\overline{c} - s\overline{d}}{p}\Big) \\
&= p\sum_{d=1}^{p}{}' e\Big(\frac{r\overline{d \mp 1} - s\overline{d}}{p}\Big) - \sum_{c=1}^{p-1} e\Big(\frac{r\overline{c}}{p}\Big) \sum_{d=1}^{p-1} e\Big(\frac{-s\overline{d}}{p}\Big) \\
&= p\sum_{d=1}^{p}{}' e\Big(\frac{[(r-s)d \pm s]\overline{d(d \mp 1)}}{p}\Big) - 1 \ll p\sqrt{p}
\end{aligned}$$

by Lemma 1. Here $\sum'$ means summation over all d with $(d,p) = 1 = (d \mp 1, p)$. Note: The first sum in the second last line is a special case of Cobeli and Zaharescu [2, Lemma 1] or Cobeli, Gonek and Zaharescu [3, Lemma 1].

4. $r \equiv s \not\equiv 0 \pmod p$. Similar to case 3. □

3. Theorem 3 when $0 < k < p/2$

Now, we try to express $T_\pm(p,k)$ as exponential sums similar to [5].

Lemma 3. *For any prime $p > 2$ and any integer $0 < k < p/2$,*

$$\begin{aligned}
T_\pm(p,k) =& \frac{1}{p^2}\sum_{m=1}^{p}\sum_{n=1}^{p} e\Big(\frac{-n}{p}\Big) \sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big) \Big[\sum_{a=1}^{p-1}\sum_{b=1}^{p-k} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big) e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big) \\
&+ \sum_{a=p-k+1}^{p-1}\sum_{b=p-k+1}^{p-1} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big) e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big)\Big].
\end{aligned}$$

Proof. We shall only prove the formula for $T_+(p,k)$; the proof for $T_-(p,k)$ is similar. Observe that $T_+(p,k) = \#\{a : 0 < a - b \le k, \overline{b} - \overline{a} = 1\}$. Thus, as

$$\sum_{n=1}^{p} e\Big(\frac{nr}{p}\Big) = \begin{cases} p, & p \mid r; \\ 0, & p \not| r, \end{cases} \tag{4}$$

$$
\begin{aligned}
T_+(p,k) =& \sum_{t=1}^{k} \sum_{\substack{a=1 \\ a-b=t, \overline{b}-\overline{a}=1}}^{p-1} \sum_{b=1}^{p-1} 1 \\
=& \frac{1}{p^2} \sum_{m=1}^{p} \sum_{n=1}^{p} \sum_{t=1}^{k} \sum_{\substack{a=1 \\ a>b}}^{p-1} \sum_{b=1}^{p-1} e\Big(\frac{m(a-b-t)}{p}\Big) e\Big(\frac{n(\overline{b}-\overline{a}-1)}{p}\Big) \\
=& \frac{1}{p^2} \sum_{m=1}^{p} \sum_{n=1}^{p} e\Big(\frac{-n}{p}\Big) \sum_{t=1}^{k} e\Big(\frac{-mt}{p}\Big) \Big[\sum_{\substack{a=1 \\ a>b}}^{p-1} \sum_{b=1}^{p-k} e\Big(\frac{ma-n\overline{a}}{p}\Big) e\Big(\frac{-mb+n\overline{b}}{p}\Big) \\
&+ \sum_{\substack{a=p-k+1 \\ a>b}}^{p-1} \sum_{b=p-k+1}^{p-1} e\Big(\frac{ma-n\overline{a}}{p}\Big) e\Big(\frac{-mb+n\overline{b}}{p}\Big) \Big]
\end{aligned} \tag{5}
$$

Note that we do not need the condition $\overline{b} > \overline{a}$ because $-p+2 \le \overline{b}-\overline{a} \le p-2$ which does not allow $\overline{b}-\overline{a} = 1-p$ (the only alternative besides 1 may be counted). Now $t-p \le k-p$. It is valid to drop the condition $a > b$ in both double sums within the brackets because $k-p < 1-(p-k) \le a-b$ and $k-p < -k < (p-k+1)-(p-1) \le a-b$ respectively (note: $k < p/2$ is used for the second chain of inequalities). Hence, only $a-b=t$ is counted even without condition $a > b$ and we have the lemma. □

Lemma 4. *For any prime $p > 2$ and any integer $0 < k < p$,*

$$
\begin{aligned}
&\sum_{m=1}^{p} \sum_{n=1}^{p} e\Big(\frac{-n}{p}\Big) \sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big) \sum_{a=1}^{p-1} \sum_{b=1}^{p-k} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big) e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big) \\
=& kp(p-k) + O(p^{5/2} \log^2 p).
\end{aligned}
$$

Proof. We separate the left hand side into three pieces according to: (i) $m = n = p$, (ii) $n = p$ and $1 \le m \le p-1$, (iii) $1 \le m \le p$ and $1 \le n \le p-1$. The left hand side of Lemma 4

$$
\begin{aligned}
=& kp(p-k) + O(p^2) + \sum_{m=1}^{p-1} \sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big) \sum_{a=1}^{p-1} \sum_{b=1}^{p-k} e\Big(\frac{\pm ma}{p}\Big) e\Big(\frac{\mp mb}{p}\Big) \\
&+ \sum_{m=1}^{p} \sum_{n=1}^{p-1} e\Big(\frac{-n}{p}\Big) \sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big) \sum_{a=1}^{p-1} \sum_{b=1}^{p-k} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big) e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big) \\
=& kp(p-k) + O(p^2) + S_1 + S_2.
\end{aligned} \tag{6}
$$

$$
S_1 \le \sum_{m=1}^{p-1} \Big| \sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big) \Big| \Big| \sum_{b=1}^{p-k} e\Big(\frac{\mp mb}{p}\Big) \Big| \le \sum_{m=1}^{p-1} \frac{1}{|\sin(\pi m/p)|^2} \ll \sum_{m=1}^{p-1} \frac{p^2}{m^2} \ll p^2 \tag{7}
$$

by summing the geometric series and $\sin \pi x \geq 2x$ for $0 \leq x \leq 1/2$. By (4),

$$\begin{aligned}
&\sum_{a=1}^{p-1}\sum_{b=1}^{p-k} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big) e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big) \\
=&\frac{1}{p}\sum_{r=1}^{p}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big) e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big) \sum_{c=1}^{p-k} e\Big(\frac{r(b-c)}{p}\Big) \\
=&\frac{1}{p}\sum_{r=1}^{p}\sum_{c=1}^{p-k} e\Big(\frac{-cr}{p}\Big) S(r \mp m, \pm n; p)\overline{S(\mp m, \pm n; p)}.
\end{aligned}$$

Hence, by Lemma 2,

$$\begin{aligned}
S_2 \ll&\frac{1}{p}\sum_{m=1}^{p}\Big|\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big)\Big| \sum_{r=1}^{p-1}\Big|\sum_{c=1}^{p-k} e\Big(\frac{-cr}{p}\Big)\Big| p^{3/2} + \sum_{m=1}^{p}\Big|\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big)\Big| p^{3/2} \\
\ll& p^{1/2}k\sum_{r=1}^{p-1}\frac{1}{|\sin(\pi r/p)|} + p^{1/2}\Big[\sum_{m=1}^{p-1}\frac{1}{|\sin(\pi m/p)|}\Big]^2 + p^{3/2}k \qquad (8) \\
&+p^{3/2}\sum_{m=1}^{p-1}\frac{1}{|\sin(\pi m/p)|} \ll p^{1/2}\Big[\sum_{m=1}^{[p/2]}\frac{p}{m}\Big]^2 + p^{3/2}\sum_{m=1}^{[p/2]}\frac{p}{m} \ll p^{5/2}\log^2 p.
\end{aligned}$$

Combining (6), (7) and (8), we have the lemma. □

Lemma 5. *For any prime $p > 2$ and any integer $0 < k < p/2$,*

$$\begin{aligned}
&\sum_{m=1}^{p}\sum_{n=1}^{p} e\Big(\frac{-n}{p}\Big)\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big) \sum_{a=p-k+1}^{p-1}\sum_{b=p-k+1}^{p-1} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big) e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big) \\
=&\frac{1}{2}pk^2 + O(p^{5/2}\log^3 p).
\end{aligned}$$

Proof. Similar to Lemma 4, we split the left hand side into three pieces which

$$\begin{aligned}
=&k^3 + O(p^2) + \sum_{m=1}^{p-1}\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big) \sum_{a=p-k+1}^{p-1}\sum_{b=p-k+1}^{p-1} e\Big(\frac{\pm ma}{p}\Big) e\Big(\frac{\mp mb}{p}\Big) \\
&+ \sum_{m=1}^{p}\sum_{n=1}^{p-1} e\Big(\frac{-n}{p}\Big)\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big) \sum_{a=p-k+1}^{p-1}\sum_{b=p-k+1}^{p-1} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big) e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big) \qquad (9) \\
=&k^3 + O(p^2) + S_1 + S_2.
\end{aligned}$$

Replacing a by $p-a$ and b by $p-b$,

$$\begin{aligned} S_1 =& \sum_{m=1}^{p-1}\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big)\sum_{a=1}^{k-1}\sum_{b=1}^{k-1} e\Big(\frac{\mp ma}{p}\Big)e\Big(\frac{\pm mb}{p}\Big) \\ =& \sum_{t=1}^{k}\sum_{a=1}^{k-1}\sum_{b=1}^{k-1}\sum_{m=1}^{p} e\Big(\frac{\pm m(b-a-t)}{p}\Big) - k^3 + O(k^2) \\ =& p\sum_{t=1}^{k}\sum_{\substack{a=1\\ b-a=t}}^{k-1}\sum_{b=1}^{k-1} 1 - k^3 + O(k^2) = \frac{1}{2}pk^2 - k^3 + O(pk) \end{aligned} \tag{10}$$

because we may count $b-a=t$ or $b-a=t-p$ but the second case is not possible as $t-p \le k-p < -k+2 \le b-a$. Here $k < p/2$ is crucial.

Applying (4) twice,

$$\begin{aligned} &\sum_{a=p-k+1}^{p-1}\sum_{b=p-k+1}^{p-1} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big)e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big) \\ =&\frac{1}{p^2}\sum_{r=1}^{p}\sum_{s=1}^{p}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big)e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big) \\ &\times \sum_{c=p-k+1}^{p-1} e\Big(\frac{r(a-c)}{p}\Big)\sum_{d=p-k+1}^{p-1} e\Big(\frac{s(b-d)}{p}\Big) \\ =&\frac{1}{p^2}\sum_{r=1}^{p}\sum_{s=1}^{p} K(r)K(s)S(s\mp m,\pm n;p)\overline{S(\mp m-r,\pm n;p)} \end{aligned}$$

where $K(x)=\sum_{n=p-k+1}^{p-1} e(-nx/p)$. Rearranging the sums and applying Lemma 2,

$$\begin{aligned} S_2 =&\frac{1}{p^2}\sum_{m=1}^{p}\sum_{t=1}^{k} e\Big(\frac{mt}{p}\Big)\sum_{r=1}^{p}\sum_{s=1}^{p} K(r)K(s) \\ &\times\sum_{n=1}^{p-1} e\Big(\frac{-n}{p}\Big)S(s\mp m,\pm n;p)\overline{S(\mp m-r,\pm n;p)} \\ \ll&\frac{1}{p^{1/2}}\sum_{m=1}^{p}\Big|\sum_{t=1}^{k} e\Big(\frac{mt}{p}\Big)\Big|\sum_{r=1}^{p}|K(r)|\sum_{s=1}^{p}|K(s)| \\ \ll&\frac{1}{p^{1/2}}\Big[k+\sum_{m=1}^{[p/2]}\frac{1}{|\sin(\pi m/p)|}\Big]^3 \ll \frac{1}{p^{1/2}}(k+p\log p)^3 \ll p^{5/2}\log^3 p. \end{aligned} \tag{11}$$

Combining (9), (10) and (11), we have the lemma. □

To prove Theorem 3 when $0 < k < p/2$, apply Lemma 4 and 5 to Lemma 3 and get

$$T_{\pm}(p,k) = \frac{1}{p^2}\Big[kp(p-k) + \frac{1}{2}pk^2 + O(p^{5/2}\log^3 p)\Big] = k - \frac{k^2}{2p} + O(p^{1/2}\log^3 p)$$

which gives Theorem 3 in that range of k.

4. Theorem 3 when $p/2 < k < p$

Before proceeding, let us introduce some notation.

$$\begin{aligned}
U_+(p,k) =& \#\{n : 0 < n < p, p-k \le \overline{n} - \overline{n+1} < p\},\\
U_-(p,k) =& \#\{n : 0 < n < p, -p < \overline{n} - \overline{n+1} \le -p+k\},\\
V_+(p,k) =& \#\{n; 0 < n < p, \overline{n} - \overline{n+1} \equiv t \pmod p \text{ for } 1 \le t \le k\},\\
V_-(p,k) =& \#\{n; 0 < n < p, \overline{n} - \overline{n+1} \equiv -t \pmod p \text{ for } 1 \le t \le k\}.
\end{aligned}$$

Then one can easily see that

$$V_+(p,k) = T_+(p,k) + U_-(p,k) \text{ and } V_-(p,k) = T_-(p,k) + U_+(p,k). \tag{12}$$

Lemma 6. *For any prime $p > 2$ and any integer $0 < k < p$,*

$$V_{\pm}(p,k) = \frac{1}{p^2}\sum_{m=1}^{p}\sum_{n=1}^{p} e\Big(\frac{-n}{p}\Big)\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big)\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big)e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big).$$

Proof. Use (4). Note: it is easier than Lemma 3 because one does not need to worry about $a > b$ or $a < b$. □

Lemma 7. *For any prime $p > 2$ and any integer $0 < k < p$,*

$$\begin{aligned}
&\sum_{m=1}^{p}\sum_{n=1}^{p} e\Big(\frac{-n}{p}\Big)\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big)\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big)e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big)\\
=& kp^2 + O(p^{5/2}\log p)
\end{aligned}$$

Proof. Similar to Lemma 4, we split the left hand side into three pieces which

$$\begin{aligned}
=& kp^2 + O(p^2) + \sum_{m=1}^{p-1}\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big)\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} e\Big(\frac{\pm ma}{p}\Big)e\Big(\frac{\mp mb}{p}\Big)\\
&+ \sum_{m=1}^{p}\sum_{n=1}^{p-1} e\Big(\frac{-n}{p}\Big)\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big)\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} e\Big(\frac{\pm ma \mp n\overline{a}}{p}\Big)e\Big(\frac{\mp mb \pm n\overline{b}}{p}\Big)\\
=& kp^2 + O(p^2) + S_1 + S_2.
\end{aligned} \tag{13}$$

By (4),

$$S_1 \le \sum_{m=1}^{p-1}\sum_{t=1}^{k} 1 \ll p^2. \tag{14}$$

After rearranging summations,

$$\begin{aligned} S_2 =& \sum_{m=1}^{p}\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big)\sum_{n=1}^{p-1} e\Big(\frac{-n}{p}\Big) S(\mp m, \pm n; p)\overline{S(\mp m, \pm n; p)} \\ \ll& p^{3/2}\sum_{m=1}^{p}\Big|\sum_{t=1}^{k} e\Big(\frac{\mp mt}{p}\Big)\Big| \\ \ll& p^{3/2}\Big[k + \sum_{m=1}^{[p/2]}\frac{1}{|\sin(\pi m/p)|}\Big] \ll p^{3/2}(k + p\log p) \ll p^{5/2}\log p \end{aligned} \tag{15}$$

by Lemma 2, summing the geometric series and $\sin(\pi x) \ge 2x$. We have the lemma by (13), (14) and (15). □

Lemma 8. *For any prime $p > 2$ and any integer $0 \le k < p/2$,*

$$U_{\pm}(p,k) = \frac{k^2}{2p} + O(p^{1/2}\log^3 p).$$

Proof. First note that when $k = 0$, $U_{\pm}(p,k) = 0$. Now assume $k > 0$. From (12), $U_{\pm}(p,k) = V_{\mp}(p,k) - T_{\mp}(p,k)$. Thus, by Lemma 6, 7 and Theorem 3 in the range $0 < k < p/2$,

$$U_{\pm}(p,k) = k + O(p^{1/2}\log p) - \Big(k - \frac{k^2}{2p} + O(p^{1/2}\log^3 p)\Big)$$

which gives the lemma. □

To prove Theorem 3 when $p/2 < k < p$, observe that $0 \le p - k - 1 < p/2$ and

$$\begin{aligned} T_{\pm}(p,k) =& T_{\pm}\Big(p, \frac{p-1}{2}\Big) + \Big[U_{\pm}\Big(p, \frac{p-1}{2}\Big) - U_{\pm}(p, p-k-1)\Big] \\ =& \frac{p-1}{2} - \frac{(\frac{p-1}{2})^2}{2p} + \Big[\frac{(\frac{p-1}{2})^2}{2p} - \frac{(p-k-1)^2}{2p}\Big] + O(p^{1/2}\log^3 p) \\ =& \frac{p}{2} - \frac{p^2 - 2pk + k^2}{2p} + O(1) + O(p^{1/2}\log^3 p) \\ =& k - \frac{k^2}{2p} + O(p^{1/2}\log^3 p) \end{aligned}$$

by Theorem 3 in the range $0 < k < p/2$ and Lemma 8.

5. Proof of Theorems 1 and 2

By Theorem 3, $T(p,k) = 2k - k^2/p + O(p^{1/2}\log^3 p)$ for integer $0 < k < p$. More generally,

$$T(p,u) = \#\{n : 0 < |\overline{n} - \overline{n+1}| \le u\} = 2u - \frac{u^2}{p} + O(p^{1/2}\log^3 p) \tag{16}$$

for any real number $0 \le u \le p$. Using the Riemann-Stieltjes integral, integration by parts, and (16),

$$\begin{aligned}
&\sum_{n=1}^{p-2} |\overline{n} - \overline{n+1}|^\lambda = \int_0^p u^\lambda \, dT(p,u) = T(p,p)p^\lambda - \lambda \int_0^p u^{\lambda-1} T(p,u) du \\
=&p^{\lambda+1} + O(p^\lambda) - \lambda \int_0^p 2u^\lambda - \frac{u^{\lambda+1}}{p} + O(u^{\lambda-1}p^{1/2}\log^3 p)\, du \\
=&p^{\lambda+1} - \Big[\frac{2\lambda}{\lambda+1}p^{\lambda+1} - \frac{\lambda}{\lambda+2}p^{\lambda+1}\Big] + O(p^{\lambda+1/2}\log^3 p) \\
=&\frac{2}{(\lambda+1)(\lambda+2)}p^{\lambda+1} + O(p^{\lambda+1/2}\log^3 p)
\end{aligned}$$

which gives Theorem 2 and hence Theorem 1.

Numerical calculations (by a C++ program) suggest that the error term in Theorem 3 is probably best possible except for the extra logarithms.

Let $m_p^{\pm} = \max_{1\le k<p} |T_{\pm}(p,k) - (k - \frac{k^2}{2p})|$.

p	101	103	107	109	113	127	131	137
$m_p^+/\sqrt{p}$	0.4951	0.6103	0.9794	0.7504	0.4595	0.9122	0.6133	0.6401
$m_p^-/\sqrt{p}$	0.5951	0.7098	0.6993	0.4956	0.4812	0.7976	0.9067	0.5416

p	5501	5503	5507	5519	5521	5527	5531	5557
$m_p^+/\sqrt{p}$	0.5786	0.6384	0.7021	0.6350	1.1337	0.4528	0.6928	0.7150
$m_p^-/\sqrt{p}$	0.5945	0.6532	0.7342	0.5888	1.0775	0.4621	0.7291	0.7530

p	12301	12323	12329	12343	12347	12373	12377	12379
$m_p^+/\sqrt{p}$	0.5249	0.6978	0.8166	1.0416	1.1251	0.6540	0.8172	0.6914
$m_p^-/\sqrt{p}$	0.5521	0.6745	0.8101	1.0346	1.1069	0.6789	0.8144	0.6778

p	60013	60017	60029	60037	60041	60077	60083	60089
$m_p^+/\sqrt{p}$	0.5172	0.7776	0.5806	0.8265	0.8441	0.9457	0.4469	0.5922
$m_p^-/\sqrt{p}$	0.5312	0.7789	0.5792	0.8411	0.8489	0.9514	0.4373	0.5897

We conclude with the following

Conjecture 1.

$$m_p^{\pm} \ll p^{1/2} \quad \textit{and} \quad m_p^{+} - m_p^{-} = o(p^{1/2}).$$

Note: After finishing this paper, we came across Cobeli and Zaharescu [2], and found that it is far more general and would give

$$T_{\pm}(p,k) = k - \frac{k^2}{2p} + O(p^{5/6}\log^{2/3} p).$$

Hence their method gives our results except for a bigger error term.

References

[1] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. **88** (1966), 71-105.

[2] C.I. Cobeli and A. Zaharescu, *The order of inverses mod q*, Mathematika **47** (2000), 87-108.

[3] C.I. Cobeli, S.M. Gonek and A. Zaharescu, *The distribution of patterns of inverses modulo a prime*, J. Number Theory **101** (2003), 209-222.

[4] C.J. Moreno and O. Moreno, *Exponential sums and Goppa codes. I*, Proc. Amer. Math. Soc. **111** (1991), no. 2, 523-531.

[5] W.P. Zhang, *On the Distribution of Inverses Modulo n*, J. Number Theory **61** (1996), 301-310.