#A51 INTEGERS 9 (2009), 699-702

A SHORT NOTE ON THE DIFFERENCE BETWEEN INVERSES OF CONSECUTIVE INTEGERS MODULO P

Tsz Ho Chan
Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, U.S.A.
tchan@memphis.edu

Received: 5/25/09, Accepted: 9/17/09, Published: 12/23/09

Abstract

In a previous paper, the author studied the distribution of differences between the multiplicative inverses of consecutive integers modulo p and raised two conjectures. In this paper, one of the conjectures is resolved by an elementary method.

1. Introduction and Main Results

In this article, p stands for an odd prime number. For any integer $0 < n < p$, $\overline{n}$ denotes the integer between 0 and p satisfying $n\overline{n} \equiv 1 \pmod{p}$. In [1], the author studied the distribution of the distances between multiplicative inverses of consecutive integers $\pmod{p}$ and showed that

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

Hence the distance between inverses of consecutive integers, $|\overline{n} - \overline{n+1}|$, is about $p/3$ on average which is what one expects if taking multiplicative inverse behaves like a random permutation. A similar study on the distribution of $|n - \overline{n}|$ was made by Zhang [3] earlier. Since multiplicative inverse $\overline{x}$ can be interpreted as the y-coordinates of the algebraic curve $f(x, y) = xy - 1 = 0$ modulo p, Zhang's work was generalized to the study of distribution of points on irreducible curves modulo p in two-dimensional space by Zheng [4] and in higher dimensional case by Cobeli and Zaharescu [2].

Going back to (1), its proof boils down to showing

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

for $0 < k < p$, where

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

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

Based on numerical evidence, it was conjectured that

$$m_p^+ - m_p^- = o(p^{1/2}),$$

where

$$m_p^+ := \max_{0<k<p} \left| T_+(p,k) - \left(k - \frac{k^2}{2p}\right) \right| \text{ and } m_p^- := \max_{0<k<p} \left| T_-(p,k) - \left(k - \frac{k^2}{2p}\right) \right|.$$

However, a closer look at the tables towards the end of [1] suggests that $m_p^+ - m_p^- = O(1)$. Indeed, we have the following:

Theorem 1. *For any integer* $0 < k < p$,

$$|T_+(p,k) - T_-(p,k)| \le 9.$$

Corollary 2. *We have*

$$|m_p^+ - m_p^-| \le 9.$$

2. Proof of Theorem 1 and Corollary 2

Proof of Theorem 1. From the definition of $T_+(p,k)$, with $a = \overline{n}$ and $b = \overline{n+1}$, we have

$$T_+(p,k) = \#\{(a,b) : 1 \le a, b \le p-1,\ \overline{b} - \overline{a} = 1,\ 0 < a - b \le k\}.$$

As $0 < \overline{a}, \overline{b} < p$,

$$\begin{aligned} \overline{b} - \overline{a} = 1 \Leftrightarrow \overline{b} - \overline{a} \equiv 1 \pmod p \quad &\Leftrightarrow a - b \equiv ab \pmod p \\ &\Leftrightarrow (a+1)(b-1) \equiv -1 \pmod p, \end{aligned}$$

we have

$$\begin{aligned} T_+(p,k) = \#\{(a,b) : 1 \le a, b \le p-1,\ (a+1)(b-1) \equiv -1 \pmod p,& \\ 0 < a - b \le k\}& \\ = \#\{(a',b') : 2 \le a' \le p-1,\ 1 \le b' \le p-2,\ a'b' \equiv -1 \,(\text{mod } p),& \\ 2 < a' - b' \le k+2\}.& \end{aligned}$$

Similarly, with $a = \overline{n+1}$ and $b = \overline{n}$, we have

$$T_-(p,k) = \#\{(a,b) : 1 \le a, b \le p-1,\ \overline{b} - \overline{a} = -1,\ 0 < a - b \le k\}.$$

As $0 < \overline{a}, \overline{b} < p$,

$$\overline{b} - \overline{a} = -1 \Leftrightarrow \overline{b} - \overline{a} \equiv -1 \pmod p \Leftrightarrow a - b \equiv -ab \pmod p \Leftrightarrow (a-1)(b+1) \equiv -1 \pmod p,$$

we have

$$\begin{aligned} T_-(p,k) &= \#\{(a,b) : 1 \le a, b \le p-1,\ (a-1)(b+1) \equiv -1 \pmod p,\ 0 < a-b \le k\} \\ &= \#\{(a',b') : 1 \le a' \le p-2,\ 2 \le b' \le p-1,\ a'b' \equiv -1 \pmod p, \\ &\qquad -2 < a' - b' \le k-2\}. \end{aligned}$$

One can see that $T_+(p,k)$ and $T_-(p,k)$ are almost the same except:

- when $a' = p-1$ and $b' = 1$ which may contribute at most one to $T_+(p,k)$.
- when $a' = 1$ and $b' = p-1$ which may contribute at most one to $T_-(p,k)$.
- when $2 \le a', b' \le p-2$ and $a' - b' = k-1,\ k,\ k+1$ or $k+2$ which may contribute at most eight to $T_+(p,k)$.
- when $2 \le a', b' \le p-2$ and $a' - b' = -1,\ 0,\ 1$ or 2 which may contribute at most eight to $T_-(p,k)$.

Here we use the fact that any quadratic polynomial has at most two solutions (mod p). Therefore $-9 \le T_+(p,k) - T_-(p,k) \le 9$. □

Proof of Corollary 2. For any $0 < k < p$, let

$$E_+(p,k) := T_+(p,k) - \Big(k - \frac{k^2}{2p}\Big) \text{ and } E_-(p,k) := T_-(p,k) - \Big(k - \frac{k^2}{2p}\Big)$$

Theorem 1 tells us that

$$-9 \le E_+(p,k) - E_-(p,k) \le 9.$$

By definition,

$$-m_p^+ \le E_+(p,k) \le m_p^+.$$

Hence

$$-m_p^+ - 9 \le E_+(p,k) - 9 \le E_-(p,k) \le E_+(p,k) + 9 \le m_p^+ + 9.$$

Thus $|E_-(p,k)| \le m_p^+ + 9$ which implies that $m_p^- \le m_p^+ + 9$ or $-9 \le m_p^+ - m_p^-$. Similarly, one can show that $m_p^+ - m_p^- \le 9$ and we have the corollary. □

Note and Acknowledgement The reference on Cobeli and Zaharescu in the end note of [1] is incorrect. The correct reference should be the paper [2] quoted in this paper. The author would like to thank the anonymous referee for helpful suggestions.

References

[1] T.H. Chan, *Distribution of differences between inverses of consecutive integers modulo p*, Integers 4 (2004), A3, 11pp. (electronic).

[2] C. Cobeli and A. Zaharescu, *On the distribution of the F_p-points on an affine curve in r dimensions*, Acta Arith. 99 (2001), no. 4, 321-329.

[3] W. Zhang, *On the distribution of inverses modulo n*, J. Number Theory 61 (1996), 301-310.

[4] Z. Zheng, *The distribution of zeros of an irreducible curve over a finite field*, J. Number Theory 59 (1996), 106-118.