ACTA ARITHMETICA
C.2 (2001)

On the distribution of inverses modulo p (II)

by

WENPENG ZHANG (Shaanxi)

1. Introduction. Let p be an odd prime. For each integer a with $0 < a < p$, we define $\overline{a}$ by the congruence equation $a\overline{a} \equiv 1 \bmod p$ and $0 < \overline{a} < p$. For any fixed positive integer k and any fixed real number $0 < \delta < 1$, Professor Andrew Granville had proposed to study the limit distribution properties of

$$\frac{1}{p-1} \sum_{\substack{a=1 \\ |a-\overline{a}|<\delta p}}^{p-1} 1.$$

The author [3] completely solved this problem, and obtained a sharp asymptotic formula. That is, we proved that

$$\sum_{\substack{a=1 \\ |a-\overline{a}|<\delta p}}^{p-1} 1 = \delta(2-\delta)p + O(p^{1/2}\ln^2 p). \tag{1}$$

In this paper, as a generalization of [3], we study the distribution properties of $|p\{a^k/p\} - p\{\overline{a}^k/p\}|$, and obtain a general asymptotic formula, where $\{x\} = x - [x]$, $[x]$ denotes the greatest integer not exceeding x. In fact, we use the J. H. H. Chalk and R. A. Smith's deep result [2], which is based on E. Bombieri's work on exponential sums [1], and the estimates for trigonometric sums to prove the following more general conclusion:

THEOREM. *Let p be an odd prime. Then for any fixed positive integer k and real number $0 < \delta < 1$, we have the asymptotic formula*

$$\sum_{\substack{a=1 \\ |\{a^k/p\}-\{\overline{a}^k/p\}|<\delta}}^{p-1} 1 = \delta(2-\delta)p + O_k(p^{1/2}\ln^2 p),$$

where O_k means that the O-constant depends only on k.

2000 *Mathematics Subject Classification*: 11N69, 11L05.
Key words and phrases: general Kloostermann's sums, distribution of inverses.
This work is supported by the N.S.F. and the P.N.S.F. of P.R. China.

From this theorem we may immediately deduce the following

Corollary. *Let p be an odd prime, k be any fixed positive integer. Then for any fixed real number $0 < \delta < 1$, we have the limit distribution formula*

$$\lim_{p\to\infty}\frac{1}{p}\sum_{\substack{a=1\\ |\{a^k/p\}-\{\overline{a}^k/p\}|<\delta}}^{p-1} 1=\delta(2-\delta).$$

Remark. Let F_p^* denote the multiplicative group formed by nonzero residue classes mod p. It is clear that the k-powers of nonzero residue classes mod p form a multiplicative subgroup, say U_k, of F_p^*. If k and $p-1$ are relatively prime, then U_k is the full group F_p^* and the result of our theorem reduces exactly to the case $k=1$, which was investigated in [3]. The new feature in this paper is when $(k,p-1)=d>1$ in which case $U_k=U_d$ is a proper subgroup of F_p^*. Thus the results of the present paper can be interpreted as results on the distribution of inverses inside a subgroup of small index in F_p^*.

2. Some lemmas. To prove the Theorem, we need several lemmas.

Lemma 1. *Let f,g be polynomials in $F_p[x,y]$ and suppose that*

(a) *$f(x,y)$ is absolutely irreducible in $F_p[x,y]$,*
(b) *$g(x,y)\not\equiv c \pmod{f(x,y)}$ in $F_p[x,y]$ for any integer c.*

Then we have the estimate

$$\sum_{\substack{a=1\\ f(a,b)\equiv 0 \,(\mathrm{mod}\, p)}}^{p}\sum_{b=1}^{p} e\left(\frac{g(a,b)}{p}\right)\ll (d_1^2-3d_1+2d_1d_2)p^{1/2}+d_1^2$$

for all primes p, where $F_p[x,y]$ denotes the set of all polynomials with coefficients in the residue systems modulo p, $d_1=d(f)$ and $d_2=d(g)$ are the degrees of f and g in $F_p[x,y]$, and $e(y)=e^{2\pi iy}$.

Proof. See [2], Theorem 2.

Lemma 2. *Let p be an odd prime, m and n be integers. Then for any fixed positive integer k, we have the estimate*

$$\sum_{a=1}^{p-1} e\left(\frac{ma^k+n\overline{a}^k}{p}\right)\ll_k p^{1/2}(m,n,p)^{1/2},$$

where (m,n,p) denotes the greatest common divisor of m, n and p.

Proof. It is clear that the assertion is true if $p\mid m$ and $p\mid n$. So without loss of generality we can assume $(m,n,p)=1$. Take $f(x,y)=xy-1$ and $g(x,y)=mx^k+ny^k$ in Lemma 1 and note that $g(x,y)\not\equiv c \pmod{f(x,y)}$ in

$F_p[x,y]$ for any integer c if $(m,n,p)=1$. Applying Lemma 1 we immediately get the estimate

$$\sum_{a=1}^{p-1} e\bigg(\frac{ma^k+n\overline{a}^k}{p}\bigg) = \sum_{\substack{a=1\\ ab\equiv 1 \pmod p}}^{p}\sum_{b=1}^{p} e\bigg(\frac{ma^k+nb^k}{p}\bigg) = \sum_{\substack{a=1\\ f(a,b)\equiv 0 \pmod p}}^{p}\sum_{b=1}^{p} e\bigg(\frac{g(a,b)}{p}\bigg) \ll_k p^{1/2}.$$

This proves Lemma 2.

Lemma 3. *Let p be an odd prime. Then for any fixed real number $0<\delta<1$, we have the estimate*

$$\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\bigg|\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} e\bigg(\frac{-rc-sd}{p}\bigg)\bigg| = O(p^2\ln^2 p).$$

Proof. First note the trigonometric identity

$$\sum_{a=1}^{n} e(ax) = e\bigg(\frac{(n+1)x}{2}\bigg)\frac{\sin \pi n x}{\sin \pi x}. \tag{2}$$

Applying (2) we have

$$\begin{aligned}
&\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\bigg|\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} e\bigg(\frac{-rc-sd}{p}\bigg)\bigg| \qquad (3)\\
&\le 2\cdot\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\bigg|\sum_{m=0}^{[\delta p]}\sum_{\substack{c=1\\ c-d=m}}^{p-1}\sum_{d=1}^{p-1} e\bigg(\frac{-rc-sd}{p}\bigg)\bigg|\\
&= 2\cdot\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\bigg|\sum_{m=0}^{[\delta p]}\sum_{d=1}^{p-1-m} e\bigg(\frac{-r(d+m)-sd}{p}\bigg)\bigg|\\
&= 2\cdot\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\bigg|\sum_{m=0}^{[\delta p]} e\bigg(\frac{-rm}{p}\bigg)\sum_{d=1}^{p-1-m} e\bigg(\frac{-(r+s)d}{p}\bigg)\bigg|\\
&\ll \sum_{r=1}^{p-1}\bigg|\sum_{m=0}^{[\delta p]} e\bigg(\frac{-rm}{p}\bigg)(p-1-m)\bigg|
\end{aligned}$$

$$+\sum_{\substack{r=1\\ r+s\neq p}}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{m=0}^{[\delta p]} e\left(\frac{-rm}{p}\right)e\left(\frac{-(r+s)}{p}\right)\frac{e\left(\frac{-(r+s)(p-1-m)}{p}\right)-1}{e\left(\frac{-(r+s)}{p}\right)-1}\right|$$

$$\ll \sum_{r=1}^{p-1}\left|\sum_{m=0}^{[\delta p]} e\left(\frac{-rm}{p}\right)(p-1-m)\right| + \sum_{\substack{r=1\\ r+s\neq p}}^{p-1}\sum_{s=1}^{p-1}\frac{1}{\left|e\left(\frac{-(r+s)}{p}\right)-1\right|}$$

$$\times\left|\sum_{m=0}^{[\delta p]} e\left(\frac{-rm-(r+s)(p-1-m)}{p}\right)-\sum_{m=0}^{[\delta p]} e\left(\frac{-rm}{p}\right)\right|.$$

Note the trigonometric sum estimate

$$\sum_{m\le M} m^k e(mx) \le M^k \min\left(M, \frac{1}{|\sin \pi x|}\right) \quad \text{for } k\ge 0. \tag{4}$$

From (3) and (4) we get

$$\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} e\left(\frac{-rc-sd}{p}\right)\right|$$

$$\ll \sum_{r=1}^{p-1}\frac{p}{\left|\sin\frac{\pi r}{p}\right|}+\sum_{\substack{r=1\\ r+s\neq p}}^{p-1}\sum_{s=1}^{p-1}\frac{1}{\left|\sin\frac{\pi(r+s)}{p}\right|}\left[\frac{1}{\left|\sin\frac{\pi r}{p}\right|}+\frac{1}{\left|\sin\frac{\pi s}{p}\right|}\right]$$

$$\ll p^2\ln p+\sum_{r=1}^{p-1}\frac{1}{\left|\sin\frac{\pi r}{p}\right|}\sum_{\substack{s=1\\ s\neq p-r}}^{p-1}\frac{1}{\left|\sin\frac{\pi(r+s)}{p}\right|}$$

$$\ll p^2\ln^2 p.$$

This proves Lemma 3.

3. Proof of the Theorem. In this section, we complete the proof of the Theorem. First note the trigonometric identity

$$\sum_{r=1}^{q} e\left(\frac{rn}{q}\right)=\begin{cases} q & \text{if } q\mid n,\\ 0 & \text{if } q\nmid n,\end{cases}$$

and the identity

$$\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left[\sum_{\substack{a=1\\ ab\equiv 1 \,(\mathrm{mod}\, p)}}^{p-1}\sum_{b=1}^{p-1} e\left(\frac{r\cdot p\left\{\frac{a^k}{p}\right\}+s\cdot p\left\{\frac{b^k}{p}\right\}}{p}\right)\right]$$

$$=\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left[\sum_{a=1}^{p-1} e\left(\frac{r\cdot a^k+s\cdot \overline{a}^k}{p}\right)\right].$$

From the estimates for trigonometric sums and Lemmas 2 and 3 we have

$$\sum_{\substack{a=1\\ |\{a^k/p\}-\{\overline{a}^k/p\}|<\delta}}^{p-1} 1$$

$$= \sum_{\substack{a=1\\ ab\equiv 1 (\bmod p)\\ |\{a^k/p\}-\{b^k/p\}|<\delta}}^{p-1}\sum_{b=1}^{p-1} 1$$

$$= \frac{1}{p^2}\sum_{r=1}^{p}\sum_{s=1}^{p}\sum_{\substack{a=1\\ ab\equiv 1\,(\bmod p)}}^{p-1}\sum_{b=1}^{p-1}\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} e\bigg(\frac{r\big(p\big\{\frac{a^k}{p}\big\}-c\big)}{p}\bigg)e\bigg(\frac{s\big(p\big\{\frac{b^k}{p}\big\}-d\big)}{p}\bigg)$$

$$= \frac{1}{p^2}\sum_{r=1}^{p}\sum_{s=1}^{p}\Bigg[\sum_{\substack{a=1\\ ab\equiv 1\,(\bmod p)}}^{p-1}\sum_{b=1}^{p-1} e\bigg(\frac{r\cdot p\big\{\frac{a^k}{p}\big\}+s\cdot p\big\{\frac{b^k}{p}\big\}}{p}\bigg)\Bigg]\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} e\bigg(\frac{-rc-sd}{p}\bigg)$$

$$= \frac{1}{p^2}\sum_{r=1}^{p}\sum_{s=1}^{p}\Bigg[\sum_{a=1}^{p-1} e\bigg(\frac{r\cdot a^k+s\cdot\overline{a}^k}{p}\bigg)\Bigg]\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} e\bigg(\frac{-rc-sd}{p}\bigg)$$

$$= \frac{1}{p^2}\sum_{a=1}^{p-1}\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} 1 + \frac{2}{p^2}\sum_{r=1}^{p-1}\Bigg[\sum_{a=1}^{p-1} e\bigg(\frac{r\cdot a^k}{p}\bigg)\Bigg]\cdot\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} e\bigg(\frac{-rc}{p}\bigg)$$

$$+ \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\Bigg[\sum_{a=1}^{p-1} e\bigg(\frac{r\cdot a^k+s\cdot\overline{a}^k}{p}\bigg)\Bigg]\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} e\bigg(\frac{-rc-sd}{p}\bigg)$$

$$= \frac{1}{p^2}(p-1)\Big[2\cdot\sum_{m=0}^{[\delta p]}\sum_{\substack{c=1\\ c-d=m}}^{p-1}\sum_{d=1}^{p-1} 1\Big] + O(1)$$

$$+ O_k\bigg(p^{-2+1/2}\cdot\sum_{r=1}^{p-1}\bigg|\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} e\bigg(\frac{-rc}{p}\bigg)\bigg|\bigg)$$

$$+ O_k\bigg(p^{-2+1/2}\cdot\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\bigg|\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1} e\bigg(\frac{-rc-sd}{p}\bigg)\bigg|\bigg)$$

$$= \frac{1}{p^2}(p-1)\Big[2\cdot\sum_{m=0}^{[\delta p]}(p-1-m)\Big] + O(1)$$

$$+ O_k\left(p^{-2+1/2}\cdot\sum_{c=1}^{p-1}(\delta p + c)\cdot\frac{1}{\left|\sin\frac{\pi c}{p}\right|}\right) + O_k(p^{1/2}\ln^2 p)$$

$$= \frac{1}{p^2}(p-1)[2p(\delta p+1) - \delta^2 p^2 + O(p)] + O_k(p^{1/2}\ln^2 p)$$

$$= p\delta(2-\delta) + O_k(p^{1/2}\ln^2 p).$$

This completes the proof of the Theorem.

Acknowledgments. The author express his gratitude to the referee for his very helpful and detailed comments.

References

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

[2] J. H. H. Chalk and R. A. Smith, *On Bombieri's estimate for exponential sums*, Acta Arith. 18 (1971), 191–212.

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

Research Center for Basic Science
Xi'an Jiaotong University
Xi'an, Shaanxi, P.R. China
E-mail: wpzhang@nwu.edu.cn

Received on 31.5.2000
and in revised form on 18.12.2000 (3829)