ACTA ARITHMETICA
102.4 (2002)

# The distribution of inverses modulo a prime in short intervals

by

S. M. Gonek, G. S. Krishnaswami and
V. L. Sondhi (Rochester, NY)

Let $\overline{\nu}$ denote the multiplicative inverse of $\nu$ modulo an odd prime $p$ and set

$$\mathcal{N} = \{\overline{\nu} \pmod{p} : M < \nu \leq M + N\},$$

where $M \geq 0$ and $N \geq 1$ are integers such that $(M, M+N] \subseteq (0,p)$. The elements of $\mathcal{N}$ are known to be well-distributed in various senses. For instance, C. Cobeli [1] has shown that the fractional parts of representatives of $\mathcal{N}$ divided by $p$ are uniformly distributed $\pmod{1}$ when $N \gg p^{1/2+\varepsilon}$.

Here we wish to study the distribution of the elements of $\mathcal{N}$ in "short" intervals $(m, m+H]$, $1 \leq m \leq p$, where $H < p$. To this end we set

$$f(m,H) = |\{n \in (m, m+H] : n \pmod{p} \in \mathcal{N}\}|$$

(here $|\ |$ denotes cardinality) and estimate

$$\mathcal{M}_k(H,p) = \sum_{m=1}^{p} (f(m,H) - HN/p)^k. \tag{1}$$

Since each element of $\mathcal{N}$ is counted in exactly $H$ of the intervals $(m, m+H]$, $1 \leq m \leq p$, the mean of $f(m,H)$ is

$$\frac{1}{p}\sum_{m=1}^{p} f(m,H) = HN/p.$$

Therefore, $\mathcal{M}_k(H,p)$ is the $k$th moment of $f(m,H)$ about its mean. Now the probability that an integer selected at random from $[1,p]$ is congruent to an element of $\mathcal{N}$ is $N/p$. Thus, if the "events" $m+h \pmod{p} \in \mathcal{N}$, $1 \leq h \leq H$, were independent, we should have

$$\mathcal{M}_k(H,p) = \mu_k(H, N/p)p,$$

2000 *Mathematics Subject Classification*: Primary 11N69; Secondary 11K31, 11K45, 11T23.

Research of the first author was supported in part by grants from the NSF and NSA.

where $\mu_k(H,P)$ is the $k$th moment of a binomial random variable $X$ with parameters $H$ and $P$. That is,

$$\mu_k(H,P) := E((X-HP)^k) = \sum_{h=1}^{H} \binom{H}{h} P^h (1-P)^{H-h}(h-HP)^k.$$

We note that $\mu_1(H,P) = 0$ and $\mu_2(H,P) = HP(1-P)$. C. Cobeli [1] has recently shown that

$$\mathcal{M}_2(H,p) = \mu_2(H,N/p)p + O(H^2 p^{1/2}\log^2 p).$$

Our main result extends this to larger values of $k$.

Theorem. *Let $k$, $N$ and $H$ be positive integers with $1 \le N, H < p$. Then*

$$\begin{aligned}\mathcal{M}_k(H,p) &= \sum_{m=1}^{p} (f(m,H) - NH/p)^k \\ &= \mu_k(H,N/p)p + O(H^k p^{1/2}\log^k p).\end{aligned}$$

Here and elsewhere, unless otherwise indicated, implied constants depend on $k$.

One can show (see Montgomery and Vaughan [3]) that for a fixed $k$,

$$\mu_k(H,P) \ll (HP)^{[k/2]} + HP$$

uniformly for $0 \le P \le 1$ and $H = 1, 2, \ldots$ Thus our theorem immediately leads to an upper bound for $\mathcal{M}_k(H,p)$.

Corollary 1. *Let $k$, $H$ and $N$ be positive integers with $1 \le H, N < p$. Then*

$$\mathcal{M}_k(H,p) \ll p(HN/p)^{[k/2]} + HN + H^k p^{1/2}\log^k p.$$

One can also show (see [3]) that

$$\mu_k = (\nu_k + o(1))(HP(1-P))^{k/2}$$

as $HP(1-P) \to \infty$, where

$$\nu_k = \begin{cases} 1\cdot 3\cdot \ldots \cdot (k-1) & \text{if } k \text{ is even,} \\ 0 & \text{if } k \text{ is odd} \end{cases}$$

denotes the moments of a normal random variable with mean 0 and standard deviation 1. Using this together with our theorem, we obtain

Corollary 2. *If $H = o(p^{1/(2k)}/\log p)$ and $(HN/p)(1-N/p) \to \infty$, then*

$$\mathcal{M}_k(H,p) = (\nu_k + o(1))p((HN/p)(1-N/p))^{k/2}.$$

Thus, $f(m,H)$ is approximately normal with mean $NH/p$ and variance $(HN/p)(1-N/p)$ in appropriate ranges of $H$ and $N$.

Our final result is an estimate for the moments of gaps between consecutive terms of $\mathcal{N}$. Let $n_1, \ldots, n_N$ be representatives of the residue classes comprising $\mathcal{N}$ lying in $(0,p)$ and arranged in increasing order. Also set

$$S_\kappa(p) = \sum_{i=1}^{N-1} (n_{i+1} - n_i)^\kappa.$$

From Corollary 1 we shall deduce

COROLLARY 3. *Let $\varepsilon$ be an arbitrarily small positive number and let $\kappa$ be any positive number less than* $3/2$. *Then*

$$S_\kappa(p) \ll N(N/p)^{-\kappa}$$

*for $1 \le N < p$ when $0 < \kappa \le 1$, and for $p^{3/(2(3-\kappa))+\varepsilon} \ll N < p$ when $1 < \kappa < 3/2$. We also have*

$$S_\kappa(p) \gg N(N/p)^{-\kappa}$$

*for $p^{3/4+\varepsilon} \ll N < p$ and all $0 < \kappa < 3/2$. In particular*, *for $0 < \kappa < 3/2$ we have*

$$S_\kappa(p) \asymp N(N/p)^{-\kappa},$$

*provided that $p^{\max\{3/4,\, 3/(2(3-\kappa))\}+\varepsilon} \ll N < p$.*

**1. Proof of the Theorem.** For the convenience of the reader we state two necessary lemmas without proof. The first, a special case of Theorem 1 in [2], depends on the Riemann hypothesis for curves.

LEMMA 1. *Let $p, N$, and $\mathcal{N}$, be as above and let $a_1, \ldots, a_s$ be distinct integers* $(\mathrm{mod}\, p)$ *with $s \le N$. Then*

$$\sum_{\substack{1 \le x \le p \\ x + a_i \,(\mathrm{mod}\, p) \in \mathcal{N} \\ (1 \le i \le s)}} 1 = p(N/p)^s + O(sp^{1/2} \log^s p)$$

*uniformly for $1 \le s \le N < p$. Here the constant implied by the $O$-term is absolute.*

A proof of our second lemma may be found in Montgomery and Vaughan [3].

LEMMA 2. *Let $\mu_k(H,P)$ be as in the Theorem. Then*

$$\mu_k(H,P) = \sum_{r=0}^{k} \binom{k}{r} (-HP)^{k-r} \biggl( \sum_{t=0}^{r} \binom{H}{t} S(r,t) t! P^t \biggr),$$

*where $S(r,t)$ denotes a Stirling number of the second kind*, *that is*, *the number of partitions of a set of cardinality $r$ into exactly $t$ non-empty subsets.*

We now proceed with the proof of the Theorem. Expanding the right-hand side of (1) by the binomial theorem and taking the sum over $m$ inside, we find that

$$\mathcal{M}_k(H,p) = \sum_{r=0}^{k} \binom{k}{r} (-HN/p)^{k-r} \sum_{m=1}^{p} f(m,H)^r. \tag{2}$$

Here we use the convention that $f(m,H)^0 = 1$ even when $f(m,H) = 0$. Let us set

$$M_r(H) = \sum_{m=1}^{p} f(m,H)^r.$$

Then we have $M_0(H) = p$, and for $r \geq 1$,

$$M_r(H) = \sum_{\substack{x_1=1 \\ x_1 \,(\mathrm{mod}\, p) \in \mathcal{N}}}^{p} \cdots \sum_{\substack{x_r=1 \\ x_r \,(\mathrm{mod}\, p) \in \mathcal{N}}}^{p} \sum_{\substack{m=1 \\ m \leq x_i \leq m+H \\ (1 \leq i \leq r)}}^{p} 1. \tag{3}$$

Let $\mathcal{B}$ be a subset of $t \leq r$ distinct elements of $[1,p)$, each of which is congruent $(\mathrm{mod}\, p)$ to some element of $\mathcal{N}$. By the definition of $S(r,t)$, the Stirling number of the second kind, we see that the number of maps from a set of cardinality $r$ onto a set of cardinality $t$ is $S(r,t)t!$. Hence, this is also the number of terms in the $r$ outer sums on the right-hand side of (3) for which $\{x_1, \ldots, x_r\} = \mathcal{B}$. We therefore obtain

$$M_r(H) = \sum_{t=1}^{r} S(r,t)t! \sum_{\substack{\mathcal{B} \,(\mathrm{mod}\, p) \subseteq \mathcal{N} \\ |\mathcal{B}|=t}} \sum_{\substack{m=1 \\ \mathcal{B} \subseteq (m, m+H]}}^{p} 1.$$

Here $\mathcal{B}$ $(\mathrm{mod}\, p) \subseteq \mathcal{N}$ means that $x$ $(\mathrm{mod}\, p) \in \mathcal{N}$ for each $x \in \mathcal{B}$. Writing

$$d(\mathcal{B}) = \max_{x_i, x_j \in \mathcal{B}} |x_i - x_j|,$$

we see that the innermost sum equals $\max(0, H - d(\mathcal{B}))$. Thus, grouping terms according to the size of $d(\mathcal{B})$ as well as $t$, we find that

$$\begin{aligned} M_r(H) &= \sum_{t=1}^{r} S(r,t)t! \sum_{d=0}^{H-1} (H-d) \sum_{\substack{\mathcal{B} \subseteq \mathcal{N} \\ |\mathcal{B}|=t \\ d(\mathcal{B})=d}} 1 \\ &= \sum_{t=1}^{r} S(r,t)t! \sum_{d=0}^{H-1} (H-d) N(t,d), \end{aligned} \tag{4}$$

say. Note that $N(1,0) = N$, while $N(1,d) = 0$ for $d > 0$. For $t > 1$, if we set

$a_1 = 0$ and $a_t = d$, then we find that

$$N(t,d) = \sum_{\substack{1 \le a_2,\ldots,a_{t-1} < d \\ a_i \text{ distinct}}} \sum_{\substack{1 \le x \le p \\ x+a_i \,(\mathrm{mod}\, p) \in \mathcal{N} \\ (1 \le i \le t)}} 1.$$

The inner sum equals $p(N/p)^t + O(tp^{1/2}\log^t p)$ by Lemma 1, and this is counted $\binom{d-1}{t-2}$ times by the outer sum. Hence, for $t > 1$,

$$N(t,d) = p\binom{d-1}{t-2}(N/p)^t + O(d^{t-2}p^{1/2}\log^t p).$$

Note that the implicit constant in the $O$-term depends on $t$, so ultimately on $k$, but not on $p$ or $d$. Using these estimates in (4), we obtain

$$\begin{aligned} M_r(H) &= HN + \sum_{t=2}^{r} S(r,t)t! \\ &\qquad \times \sum_{d=0}^{H-1}(H-d)\left(p\binom{d-1}{t-2}(N/p)^t + O(d^{t-2}p^{1/2}\log^t p)\right) \\ &= HN + p\sum_{t=2}^{r} S(r,t)t!\,(N/p)^t \sum_{d=0}^{H-1}(H-d)\binom{d-1}{t-2} \\ &\qquad + O(H^r p^{1/2}\log^r p) \end{aligned}$$

for $r \ge 1$. Here it is to be understood that if $r = 1$ the sum vanishes.

The sum over $d$ may be evaluated using the relation $\binom{i}{j} = \frac{i}{j}\binom{i-1}{j-1}$ and the identity

$$\binom{0}{j} + \binom{1}{j} + \ldots + \binom{l}{j} = \binom{l+1}{j+1}.$$

From these we find that

$$\sum_{d=0}^{H}(H-d)\binom{d-1}{t-1} = \binom{H}{t},$$

so that

$$M_r(H) = HN + p\sum_{t=2}^{r} S(r,t)t!\,(N/p)^t\binom{H}{t} + O(H^r p^{1/2}\log^r p).$$

As $S(r,1) = 1$ for $r \ge 1$, we can include the term $HN$ in the sum by beginning it at $t = 1$. Moreover, since $S(r,0) = 0$ for $r \ge 1$, we may add the term $t = 0$ in as well. Thus, we find that when $r \ge 1$,

$$M_r(H) = p\sum_{t=0}^{r} S(r,t)t!\,(N/p)^t\binom{H}{t} + O(H^r p^{1/2}\log^r p). \tag{5}$$

Finally, using the convention $S(0,0)=1$ and recalling our initial observation that $M_0(H)=p$, we see that (5) actually holds for $r\ge 0$.

Using this in (2) and then applying Lemma 2, we obtain

$$\begin{aligned}\mathcal{M}_k(H,p) &= p\sum_{r=0}^{k}\binom{k}{r}(-HN/p)^{k-r}\sum_{t=0}^{r}\binom{H}{t}S(r,t)t!\,(N/p)^t\\ &\quad + O(H^k p^{1/2}\log^k p)\\ &= p\mu_k(H,N/p)+O(H^k p^{1/2}\log^k p).\end{aligned}$$

This completes the proof of the Theorem.

**2. Proof of Corollary 3.** To prove Corollary 3 we modify an argument of Montgomery and Vaughan [3]. Set

$$D(x)=\sum_{\substack{i=1\\ n_{i+1}-n_i>x}}^{N-1} 1.$$

Then we have

$$S_\kappa(p)=\kappa\int_0^p D(x)x^{\kappa-1}\,dx. \tag{6}$$

We first establish the upper bound. For $0\le x\le 4p/N$ we use the trivial estimate $D(x)\le N$ and find that

$$\kappa\int_0^{4p/N} D(x)x^{\kappa-1}\,dx\le N(4p/N)^\kappa \ll N\left(\frac{N}{p}\right)^{-\kappa}. \tag{7}$$

We bound $D(x)$ for larger $x$ by noting that if $n_{i+1}-n_i>H$, then

$$\sum_{\substack{m<n<m+H\\ n\,(\mathrm{mod}\,p)\in\mathcal{N}}} 1-HN/p=-HN/p$$

for $n_i\le m<n_{i+1}-H$. Thus, if $k$ is a non-negative integer, we have

$$\sum_{\substack{i=1\\ n_{i+1}-n_i>H}}^{N-1}(n_{i+1}-n_i-H)(HN/p)^{2k}\le \mathcal{M}_{2k}(H,p). \tag{8}$$

Now suppose that $HN\ge p$. Then by Corollary 1 the right-hand side of (8) is

$$\ll p(HN/p)^k+H^{2k}p^{1/2}\log^{2k} p.$$

Moreover, by the definition of $\mathcal{M}_k(H,p)$ this also holds when $k=0$. On the other hand, taking $H = [x/2]$, we see that the left-hand side of (8) is

$$\geq \sum_{\substack{i=1 \\ n_{i+1}-n_i>x}}^{N-1} (n_{i+1} - n_i - H)(HN/p)^{2k} \geq H(HN/p)^{2k} D(x).$$

Thus, for $x \geq 4p/N$ we find that

$$D(x) \ll N(xN/p)^{-k-1} + (N/p)^{-2k} x^{-1} p^{1/2} \log^{2k} p.$$

Suppose first that $0 < \kappa < 1$. Taking $k = 0$ in the above, we obtain

$$\int_{4p/N}^{p} D(x)\, x^{\kappa-1}\, dx \ll p \int_{4p/N}^{p} x^{\kappa-2}\, dx \ll N(N/p)^{-\kappa}, \tag{9}$$

for $1 \leq N < p$. On the other hand, if $\kappa > 1$, we choose $k$ large enough so that $k + 1 > \kappa$ (so, in particular, $k \geq 1$), and obtain

$$\begin{aligned} \int_{4p/N}^{p} D(x)\, x^{\kappa-1}\, dx &\ll N(N/p)^{-k-1} \int_{4p/N}^{p} x^{\kappa-k-2}\, dx \\ &\quad + (N/p)^{-2k} p^{1/2} \log^{2k} p \int_{4p/N}^{p} x^{\kappa-2}\, dx \\ &\ll N(N/p)^{-\kappa}(1 + (N/p)^{\kappa-2k-1} p^{\kappa-3/2} \log^{2k} p). \end{aligned}$$

Hence, we deduce in this case also that

$$\int_{4p/N}^{p} D(x) x^{\kappa-1}\, dx \ll N(N/p)^{-\kappa}, \tag{10}$$

provided that

$$p^{\frac{2k-1/2}{2k-\kappa+1}} \log^{\frac{2k}{2k-\kappa+1}} p \leq N < p \quad \text{and} \quad k+1 > \kappa.$$

Note that in order for the $N$-range to be non-trivial when $k \geq 1$, we must have $\kappa < 3/2$. Thus, upon combining (6), (7), (9) and (10), we find

$$S_\kappa(p) \ll N(N/p)^{-\kappa} \tag{11}$$

for $1 \leq N < p$ if $0 < \kappa < 1$, and for $p^{\frac{2k-1/2}{2k-\kappa+1}} \log^{\frac{2k}{2k-\kappa+1}} p \leq N < p$ if $1 < \kappa < 3/2$, where $k$ is any integer such that $k+1 > \kappa$. When $1 < \kappa < 3/2$, we achieve the largest $N$-range by minimizing the exponent

$$\frac{2k - 1/2}{2k - \kappa + 1} = 1 - \frac{3/2 - \kappa}{2k - \kappa + 1}$$

of $p$ subject to $k + 1 > \kappa$. The minimum clearly occurs when $k = 1$, so we obtain (11) for $p^{3/(2(3-\kappa))} \log^{2/(3-\kappa)} p \leq N < p$. Finally, we note that when $\kappa = 1$, (11) follows from the definition of $S_1(p)$ for any $N$ such that $1 \leq N < p$. This gives the upper bound stated in Corollary 3.

To treat the lower bound we again consider the cases $0 < \kappa < 1$ and $\kappa \geq 1$ separately. First suppose that $\kappa \geq 1$. By Hölder's inequality we have

$$S_1(p)^\kappa \leq N^{\kappa-1} S_\kappa(p), \tag{12}$$

and we require a lower bound for $S_1(p) = n_N - n_1$. By Lemma 1 with $s = 2, a_1 = 0$, and $a_2 = (p-1)/2$, say, it follows that there is a pair of elements of $\mathcal{N}$ that are $\gg p$ apart, provided that $N \gg p^{3/4} \log p$. Hence $S_1(p) \gg p$ for such $N$, and we deduce from (11) that

$$S_\kappa(p) \gg N\left(\frac{N}{p}\right)^{-\kappa}.$$

For $0 < \kappa < 1$ we apply Hölder's inequality in the form

$$S_1(p)^q \leq S_\kappa(p)(S_{(q-\kappa)/(q-1)}(p))^{q-1},$$

where $q$ is any real number greater than 1. We have $S_1(p) \gg p$ when $N \gg p^{3/4} \log p$, as before, and also the upper bound

$$S_{(q-\kappa)/(q-1)}(p) \ll N(N/p)^{-(q-\kappa)/(q-1)}$$

for $1 < (q-\kappa)/(q-1) < 3/2$ and $p^{\frac{3}{2}(3-\frac{q-\kappa}{q-1})+\varepsilon/2} \ll N < p$. It therefore follows, on taking $q$ sufficiently large, that

$$S_\kappa(p) \gg p^q/(N^{q-1}(N/p)^{\kappa-q}) = N(N/p)^{-\kappa}$$

for $p^{3/4+\varepsilon} \ll N < p$. This gives the required lower bound.

The final assertion of the corollary follows immediately on combining the upper and lower bounds for $S_\kappa(p)$.

## References

[1] C. I. Cobeli, *Topics in the distribution of inverses* (*mod q*), doctoral dissertation, University of Rochester, 1997.

[2] C. I. Cobeli, S. M. Gonek and A. Zaharescu, *The distribution of inverses modulo a prime*, to appear.

[3] H. L. Montgomery and R. C. Vaughan, *On the distribution of reduced residues*, Ann. of Math. 123 (1986), 311–333.

Department of Mathematics
University of Rochester
Rochester, NY 14627, U.S.A.
E-mail: gonek@math.rohester.edu

*Received on 30.10.2000* (3907)